PART I - SECTION C
SCOPE OF WORK

1. MEJORAS AL ENLACE DE VOZ DE ATS (MEVA) III NETWORK

1.1 INTRODUCTION

This Statement of Work (SOW) sets forth the requirements for the MEVA III Network. MEVA III is an international collaboration by States, Territories, and International Organizations of the Central Caribbean and Central America Region jointly with the Federal Aviation Administration (FAA) to fulfill all aeronautical telecommunications requirements of the region as described in the MEVA III Document of Agreement and this SOW. The full range of technical requirements is defined in the MEVA III specification. In addition, the MEVA III contract will include engineering support services.

When the MEVA III network is fully implemented, it will provide a totally integrated C-band VSAT/TDMA/Frame Relay satellite solution that will meet or exceed all of the requirements of the MEVA member states.

1.2 BACKGROUND

In June 2013, the ICAO TCB office in Montreal, on behalf of the MEVA Technical Management Group (TMG), issued a Request for Proposal (RFP) to vendors in the VSAT telecommunication services industry, inviting submission of technical and cost proposals for MEVA III VSAT telecommunications services.

The MEVA III RFP accompanying the tender announcement specified the requirements for a set of highly reliable, satellite-based voice and data communication services that are required to support air traffic control and coordination in the Central Caribbean region through 2015.

TMG representatives from the participating MEVA member states and organizations evaluated the technical and cost proposals submitted in response to the RFP and determined the winning vendor based on a set of technical and financial criteria. Each MEVA member is responsible for signing a separate contract with the winning vendor, based on the TMG-selected proposal, for member-specific MEVA III service and support.

1.3 MEVA III CONTRACT OBJECTIVES

The primary objective of the MEVA III contract is to provide a total end-to-end telecommunications service solution for MEVA III users that minimize the cost of ownership and operation while at the same time meeting all of the FAA's functional and performance requirements.

The MEVA III network will replace the existing MEVA II TDMA network, which is now nearing the end of its useful design life, with a more technologically advanced and operationally efficient C-band VSAT MF/TDMA satellite service solution.

In order to minimize the upfront investment cost to MEVA users for converting MEVA II from TDMA operation to MF/TDMA operation, the Contractor must maximize the use of existing MEVA II equipment (e.g., dish antenna systems, RF transceivers, spares, and related indoor equipment) wherever possible.

In those cases where new equipment is to be supplied by the Contractor in order to meet service requirements, only commercial-off-the-shelf (COTS) equipment and/or software from the manufacturers and suppliers proposed by the Contractor will be used. In addition, a Service Level Agreement (SLA) has been incorporated into the contract with credits for not meeting performance requirements to ensure that certain minimum levels of service are maintained.

As stated in the MEVA III RFP, the Contractor must be capable of providing communications circuit connectivity between designated VSAT nodes in the MEVA III network and nodes in the REDDIG VSAT network in South America. The stated service solution will use the IS-14 satellite and compatible MF/TDMA terminal equipment, which is to be supplied, installed and maintained by the Contractor.

The MEVA III network must be capable of supporting future service requirements of the CAR/SAM region and sub-regions with circuit transmission services compatible with the requirements of AMHS, ATN, CPDLC, GNSS, and RADAR Data Sharing.

The Contractor is required to provide transmission services within the MEVA III network that are compatible with new and evolving network protocols and for cost effectively increasing network growth and the traffic handling capacity of the MEVA III VSAT system.

The MEVA III must have a migration path to become compliant with HSPD-12.

1.4 Scope

1.4.1 MEVA III Services

The scope of the MEVA III network contract includes all services necessary to satisfy FAA satellite-based voice and data end-to-end communications and related engineering service requirements to support air traffic control and coordination in the Central Caribbean and Central American region for the life of the contract. The geographic scope includes FAA facilities at the Atlanta (GA) NEMC, the Miami (FL) ARTCC, and the San Juan (PR) CERAP. As directed by the FAA, the Contractor may also be required to interface with system integration contractors, equipment manufacturers, airport personnel, and various FAA and U.S. Government Organizations.

1.4.2 Use of FAA-Owned Assets

The scope of this contract includes the use and incorporation of the existing VSAT dish antenna, antenna mount/pedestal and LNB (Low-Noise Block) in Atlanta and San Juan, COMSOFT´s Teleport environment as uplink station in Miami, redundant terrestrial interconnection and

Uninterruptible Power Supply (UPS) into the Contractor's network as is reasonable and practical.

In particular, these FAA-owned assets will be reused, serviced, and maintained by the Contractor to the maximum extent possible. A physical inspection of each MEVA site must be performed to determine the extent of the equipment replacement requirements (taking into consideration the age of the equipment) and identify any associated replacement costs to the FAA.

The Contractor must make maximum use of the existing RF Terminal Outdoor Unit (ODU) equipment (i.e., CODAN C-band RF transceivers, etc.) at MEVA sites. Where this is not entirely practical, the Contractor must propose an alternative equipment solution and present this information to the FAA as soon as possible after completion of the physical site survey.

The Contractor must make maximum use of the existing MEVA VSAT antenna systems (dish antenna, feed assembly, LNB, etc.) at MEVA sites. Where this is not technically practical or cost effective, the Contractor must propose an alternative solution to the FAA.

2 APPLICABLE DOCUMENTS

2.1 GENERAL

The documents listed in this section are cited in other sections of this SOW. While an extensive effort has been made to ensure the completeness of this list, document users are cautioned that they must meet all specified requirements documents cited in this SOW, whether or not they are listed below.

2.1.1 Government Documents

The Contractor must adhere to all policies and procedures established by the government. Such policies and procedures are contained in the most current version of the Government documents listed below. Unless specifically identified, the issue of a document that is cited in this SOW is the one (including all change pages, amendments, inserts, supplemental reports, etc.) that is current at the time of contract award. It must be the responsibility of the Contractor to obtain this documentation. The Contractor must advise the Government if assistance is required to obtain FAA documentation described below.

Table 2-1 Government Documents

Identifier	Title
FAA-G-2100H	Electrical Equipment General Requirements
FAA-G-1375c	Spare Parts Peculiar for Electronic, Electrical, and Mechanical Equipment
FAA STD-019d	Lightning Protection, Grounding, Bonding and Shielding

Identifier	Title
	Requirements for Facilities
FAA STD-020a	Lightning Protection, Grounding, Bonding and Shielding Requirements for Facilities
FAA STD-021a	Preparation of Interface Documentation
FAA Order 1270.1	Freedom of Information Act Program
FAA Order 1370.79A	Internet Use Policy
FAA Order 1370.81A	Electronic Mail
FAA Order 1370.82A	Information Systems Security Program
FAA Order 1370.89	Information Operations Conditions
FAA Order 1370.92A	Password and PIN Management
FAA Order 1370.114	Implementation of FTI Services and Information Security Requirements in the NAS
FAA Order 1600.1D	Personnel Security Program
FAA Order 1600.6C	Physical Security Management Program
FAA Order 1600.69	FAA Facility Security Management Program
FAA Order 1600.72	Contractor and Industrial Security Program
FAA Order 1600.73	Contractor and Industrial Security Program Operating Procedures
FAA Order 1600.75	Protecting Sensitive Unclassified Information
FAA Order 1800.66	Configuration Management Policy
FAA Order 6950.15b	ARTCC Critical Load Circuit Configuration
FAA Order 6580.3	Remote Communication Facility Installation Handbook
FAA Order 1370.92A	Password and PIN Management
FIPS Pub 112	Password Usage (www.nist.gov)
FIPS Pub 199	Standards for Security Categorization of Federal Information and Information Systems
FIPS Pub 200 (DRAFT)	Minimum Security Requirements for Federal Information and Information Systems
DOT H 1350.2	Departmental Information Resource Management Manual (DIRMM)
HR 3844	Federal Information Security Management Act of 2002 (FISMA)
OMB Circular A-130,	

Identifier	Title
Appendix III	
Public Law 100-235	Computer Security Act of 1987
Presidential Decision Directive (PDD) 63	Critical Infrastructure Protection
HSPD 12	Policy for a Common Identification Standard for Federal Employees and Contractors (http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html)

3 FAA furnished Items and Services

The FAA will provide the Contractor with the following items and services at FAA facilities in support of MEVA III on a mutually agreeable schedule.

3.1 Facilities

Space inside a Government Designated Facility

The FAA will provide the demarcation equipment to which all MEVA III services will be connected.

The amount of internal floor space at facilities that will be available for use in on-site maintenance activities, equipment storage, and related purposes must be determined during site surveys and must be subject to FAA coordination and approval.

Space Outside a Government Designated Facility

Outdoor space may be available for the installation of MEVA resources if internal facility space is not available. Where outside enclosures are available, the FAA may provide space for installation of MEVA services.

3.2 Security

Access to FAA sites will be determined on a case-by-case basis. The FAA is not responsible for physical security external to those sites (e.g. conduits from Government facilities to commercially provided rights-of-way or lines routed from buildings to commercially owned telephone poles).

3.3 Equipment

Cabling

The FAA will provide all cabling on the FAA side of the demarcation unless otherwise specified.

4 Government Responsibilities

4.1 Role of Program Management Office

The FAA MEVA III Program Manager (PM) will manage the MEVA III program and be the primary focal point for the MEVA III Contractor to interface with during the contract period of performance. The PM will perform all necessary coordination with FAA organizations, agencies and Government contractors during the implementation of MEVA services. The FAA will be responsible for the removal of any FAA-owned equipment displaced by the introduction of MEVA III service unless otherwise ordered via task order. The FAA, with Contractor support will be responsible for managing and conducting all activities necessary to obtain MEVA III Security Authorization required by FAA Order 1370.82A.

4.2 Role of Site representative (SR)

The Government will identify a Site Representative (SR) for each site. The SR will be responsible for coordinating all implementation activities through the acceptance of all implemented services.

The responsibilities of a SR include the following:

a) Serve as the FAA's local point of contact for site-related implementation activities
b) Assist the Contractor during the FAA location inventory or site survey
c) Assist the Contractor in coordinating with the appropriate government offices and other Contractor(s) who are providing that location with other telecommunications services
d) Monitor on-site installation and testing as performed by the Contractor.

4.3 Site Preparation Activities

The FAA will perform all work necessary inside and on the interior and exterior walls of FAA buildings to prepare each site for the receipt of contractor provided and installed equipment, unless otherwise ordered. As ordered by task order, the Contractor must perform site work in specified FAA facilities to prepare that site for the installation of Contractor supplied and installed equipment.

4.4 Cutover Activities

The FAA will be responsible for:

a) Cross-connecting the MEVA III to the FAA equipment on the FAA side of the demarcation point

b) Connecting Contractor-provided power lines to FAA power panels or duplex outlets.
c) Connecting Contractor-provided electrical ground lines to FAA-provided electrical ground buses.

These cutover actions will be performed at times of least interruption to FAA operations.

4.5 Test Activities

The FAA will participate in any test activity involving the interfaces by operating and maintaining the FAA systems providing these interfaces, and by supporting all mutually agreed test scenarios with system operators. The FAA's responsibilities will include:

a) Scheduling access to resources.
b) Supporting conduct of Contractor test activities.
c) Supporting resolution of problems encountered during test activities.

5 REQUIREMENTS

5.1 The Contractor must provide all necessary services and resources to design, implement, manage, control, operate and maintain the infrastructure that will provide the required MEVA III telecommunications and engineering services in accordance with this SOW and the MEVA III RFP. This includes labor, equipment, materials and real estate (if not government furnished).

Contractor responsibilities include the following:

a) The Contractor must design the MEVA III network using new commercial-off-the-shelf (COTS) equipment (defined to include hardware, software, and firmware) and existing available services.
b) The Contractor must provide telecommunications services that meet the performance parameters specified in the MEVA III RFP.
c) The Contractor must provide resources necessary to execute all Engineering Services required by this contract.
d) The Contractor must manage, engineer, configure, install, verify, implement, operate, and maintain the MEVA III network.
e) The Contractor must support the FAA certification and authorization process in accordance with FAA Order 1370.82A, *Information Systems Security Program*. Such support must include supporting technical meetings, supporting FAA security testing, delivering required security documentation identified in this SOW, and providing support to the FAA in developing the Security Certification and Authorization Package (SCAP).

5.2 PROGRAM MANAGEMENT

Program Office

The Contractor must establish a Program Office and perform program management to support and manage MEVA III services throughout the life of the contract. This includes attendance at meetings or participating in teleconferences scheduled by FAA as well as meetings or teleconferences scheduled by ICAO or the MEVA TMG. Participation at such meetings and teleconferences will be at the expense of the Contractor.

Monthly Status Report

The Contractor must report the status of the program in a Monthly System Status Assessment and Performance Report (CDRL A0001). This report must include FAA's bandwidth usage detailed per site, call record details, system performance statistics, a trouble log summary (at minimum, trouble ticket number, transaction date/time, trouble reported, cause and repair, and technician name at both ends), and any security incident.

PROGRAM MANAGEMENT ORGANIZATION

5.2.1.1 The Contractor must establish clear and effective lines of authority, coordination, communication, and accountability between the contractor's MEVA III Program Office and the FAA.

5.2.1.2 The FAA Program Management Office must have clear, timely, and effective access to levels of management within the Contractor's organization that have authority to ensure that sufficient and timely resources are available for the MEVA III services and timely attention is given to the resolution of any problems that may arise.

5.2.1.3 The Contractor must be responsible for management and control of all subcontractors/team members to ensure compliance with all requirements of the contract.

PROGRAM MANAGEMENT REVIEWS

5.2.1.4 The Contractor must be available in person or via teleconference to review the Monthly System Status Assessment and Performance Report as necessary.

5.3 TELECOMMUNICATIONS SERVICE

The Contractor must provide a total, leased end-to-end, telecommunications service solution for MEVA III users that will minimize the cost of ownership and operation while at the same time meeting all of the functional and performance requirements specified in this contract.

The Contractor must coordinate with local FAA officials and accomplish the upgrade and transition of the present MEVA II Network from the use of TDMA technology to a fully mesh capable, MF/TDMA technology network architecture. The Contractor must coordinate these activities with local FAA authorities in order to assure minimal disruption to on-going air traffic control communications services presently supported by the MEVA II Network.

The Contractor must constantly monitor and control the MEVA III network through the Contractor's Network Control Center (NCC) and backup NCC.

The Contractor must provide a MEVA III telecommunications network service that is capable of using a wide variety of standard information protocols such as X.25, IP, and circuit switching protocols for future ATN support.

The Contractor's service must permit MEVA III end-users to have access to network health data through a dedicated device. Alternatively this data can be made available online via a password protected Internet web site managed by the Contractor for this purpose. Passwords must be in accordance with FAA Order 1370.92A *Password and PIN Management Policy*. The Contractor must establish an Internet web-based database of information that will include, as a minimum, a current report of network status, user call records and statistics, trouble reports and troubleshooting activities associated with the MEVA III network (CDRL A0002).

5.4 MODIFICATION AND UPGRADING OF MEVA NETWORK SYSTEM COMPONENTS

The Contractor must modify or upgrade all the MEVA VSAT terminals at FAA sites as required for MF/TDMA operation. No equipment must be removed from FAA premises without express consent of the FAA MEVA Program Manager.

5.5 MEVA III WEBSITE

The Contractor must develop and operate/maintain an access-controlled website during the entire operation of the MEVA III network (CDRL A0002). The website must allow FAA users to see, in real-time, the information available to the NOC monitoring program, as well as call records, monthly reports, system documentation, and other documents pertinent to the MEVA III Network. A layout and description of the proposed website solution should be provided by the Contractor.

5.6 SECURITY REQUIREMENTS

General – Security services and equipment to satisfy the following requirements will be fully justified and priced as described in accordance with the service level agreement.

The Contractor must implement, operate and maintain security functions and conduct security assurance activities to protect MEVA III as required by the provisions of this contract.

The Contractor must use management and technical controls to ensure that MEVA III security is protected as required by the provisions of this contract.

The Contractor must not permit interconnection between MEVA III and non-MEVA III traffic without formal FAA MEVA III Program Office approval in advance and comply with FAA Order 1370.114, *Implementation of FTI Services and Information Security Requirements in the NAS*.

The Contractor must comply with verbal or written requests only from authorized persons from the MEVA III Program Office only to activate or revoke security credentials for access privileges. All verbal requests will be formally confirmed within five business days.

The Contractor must disable inactive user accounts (Operating System and Application) automatically after 90 days of inactivity.

The Contractor must enforce a limit of 5 consecutive invalid attempts within a 20 minute period.

The Contractor must deactivate temporary accounts that are no longer required and individual accounts of terminated or transferred users within three business days following the change in account access needs. The Contractor must change the group account authenticators (i.e., shared passwords) for terminated or transferred users within three business days following the change.

The Contractor must review system level user accounts (Operating System and Application) semi-annually and group accounts quarterly and must initiate required actions (e.g., deactivate, change access rights/privileges) based upon the review.

The Contractor must employ automated mechanisms (e.g., Active Directory, TACACS, LDAP) to support the management (e.g., establishing, activating, modifying, deactivating, reviewing, and monitoring accounts; expiring unused accounts) of system accounts.

The Contractor must accomplish access activation, delivery of credentials and any necessary access software, firmware or hardware within 5 business days after notification.

The Contractor must employ the concept of least privilege (assign and enforce the most restrictive set of rights/privileges, including system information input restrictions) when establishing system user accounts (Operating System and Applications).

The Contractor must implement system data flow control device(s) (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers), configuration settings, and rules sets that restrict system information flow as defined in the System Design Document (SSD).

The Contractor must configure MEVA III system assets to either automatically:

5.6.1.1 (1) lock the account for 20 minutes or

5.6.1.2 (2) lock the account until released by an administrator, when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.

The Contractor must, prior to granting system access, display a warning banner as part of every system login, even when systems are accessible from other systems. For example, the banner could read:

This is a COMSOFT computer system. Unauthorized access or use is a violation of international law and may result in criminal or civil proceedings. If you cause a technical disruption of the system, you agree to be responsible for the costs of restoration and any civil or criminal penalties. All activity will be monitored to ensure appropriate use. Your

continued use constitutes consent to monitoring and the system's terms of use. If you do not consent to monitoring or the terms of use, you should exit this system.

The Contractor must display the warning banner on the screen until users take explicit actions to acknowledge the notification.

The Contractor must prevent further access to the system by initiating a session lock (e.g., password protected screen saver) for local access sessions after 15 minutes of inactivity.

The Contractor must retain the session lock until the user re-authenticates.

The Contractor must allow remote access connections to the system after approval from the MEVA III Program Office (prior to connection) via the configuration management process as documented in the MEVA III SSP (CDRLA0003). The Contractor must ensure that all remote access connections made to the system follow the formal Configuration Management approval processes.

The Contractor must generate audit records for MEVA III system assets that contain the type of event, date, time, system source or subsystem asset where the event occurred, user/subject identification, outcome of the event (success/failure), and session ID if applicable. The list of assets that can produce a log and therefore audit records is as follows:

1. Satellite Modem

2. Multiplexer

The Contractor must ensure that MEVA III System audit records do not contain sensitive information, such as passwords, actual system data, or privacy information.

The Contractor must allocate sufficient storage capacity to store 14 days of security-relevant audit records in electronic format. MEVA III system auditing capacity must be configured as to reduce the likelihood of audit record storage capacity being exceeded (e.g., provide 25% capacity above estimated need).

The Contractor must configure MEVA III Systems to alert the Network Operation Center (NOC) in the event of an audit processing failure (e.g. software/hardware errors, failure in audit capturing mechanisms, audit storing capacity being reached or exceeded).

The Contractor receiving MEVA III alerts must take the following actions based on receiving an audit processing failure alert:

(1) When there is a failure in the system event generation /audit capturing mechanism; the system administrator must perform a controlled restart of the system or a controlled restart of the auditing mechanism.

(2) Follow system-level procedures for audit storage capacity being reached or exceeded.

The Contractor must provide an audit reduction and report capability (i.e. the data recorded must be searchable and have an export capability for report generation.

The Contractor must provide accurate time stamps (including date, time, and UTC offset) in audit records.

The Contractor must synchronize internal clocks every 24 hours with a common time source.

The Contractor must generate a record of each approved configuration-controlled change to the MEVA III system(s).

The Contractor must retain records of approved configuration-controlled changes to the MEVA III system.

The Contractor must implement and maintain mandatory configuration settings for information technology products employed within the system using the highest rated checklists provided on the NIST National Checklist Program site (http://web.nvd.nist.gov/view/ncp/repository) including required security patches, malicious code signature updates and spam protection updates.

The Contractor must ensure that the system components defined in the System Design Document (SSD) inventory are placed under configuration management.

The Contractor must ensure that authenticator strength (i.e., length, complexity) are at least thirteen characters in length, containing at least one upper case letter, one lower case letter, one number, and one special character (e.g., !, @, #, %, etc.).

The Contractor must change default authenticators upon system installation.

The Contractor must configure MEVA III systems to:

(1) Change/refresh authenticators containing less than 13 characters every 90 days,

(2) Require that at least one character must be changed, and

(3) Prevent password reuse for at least 10 password change cycles.

The Contractor must protect authenticator content (passwords, PIN) from unauthorized disclosure and modification in storage and in transmission.

The Contractor must obscure feedback of authentication information (e.g., masking passwords, prohibit passwords from being displayed) during the authentication process to protect the information from possible unauthorized exploitation/use.

Security Authorization

5.6.1.3 The Contractor must support activities necessary to achieve and sustain MEVA III Security Authorization by the Government Authorizing Official (AO) in accordance with FAA Order 1370.82A.

5.6.1.4 The Security Authorization must include:

a) The MEVA III equipment installation at all FAA locations from the Satellite Antenna to the FAA demarcation point.

b) The MEVA III Website discussed in section 5.5
c) The Network Management Capability

The Contractor must formally certify that all MEVA III security requirements have been fully satisfied in accordance with all applicable standards

The contractor must deliver a Systems Security Plan (SSP) (CDRL A0003),

The contractor must deliver a System Characterization Document (SCD) (CDRL A0004),

The contractor must deliver an Information Systems Contingency Plan (ISCP) (CDRL A0014) and an ISCP Test Plan and Results Report (CDRL A0015).

The Contractor must review the FAA's Security Authorization documentation for accuracy, and will provide fully justified time and cost estimates to complete remediation efforts.

Personnel Security

5.6.1.5 The Contractor must comply with the personnel security requirements as specified in FAA Order 1600.1E, *Personnel Security Program* and FAA Order 1600.72 *Contractor and Industrial Security Program*.

5.6.1.6 The Contractor must ensure that personnel who occupy positions designated as computer/automated data processing sensitive must be appropriately cleared and granted access prior to occupying such a position, in accordance with Clause 3.14-2 of Section I.

5.6.1.7 The Contractor must retrieve all security-related and system-related property upon employee termination.

Physical Security Requirements

Government Facilities

5.6.1.8 The Contractor must comply with site-specific physical security requirements, procedures, and processes established by the FAA in accordance with FAA Order 1600.6E and FAA Order 1600.69B, *FAA Facility Security Management Program*.

Non-Government Facilities

5.6.1.9 Within facilities where systems providing MEVA III services are developed, housed, or operated, the Contractor must implement physical security measures as required to ensure that specified security requirements are not compromised.

5.6.1.10 The Contractor must verify individual access authorizations before granting access to the Service Provider's facilities where the MEVA III systems are located.

5.6.1.11 The Contractor must control entry to the facility containing the MEVA III systems using physical access devices and/or guards.

5.6.1.12 When MEVA III system assets are in publicly accessible areas the Contractor must protect physical access to the MEVA III system assets.

5.6.1.13 The Contractor must monitor physical access to the MEVA III systems to detect and respond to physical security incidents.

Site Inspections

5.6.47.1 As ordered via task order, the Contractor must support Government and/or Contractor site inspections conducted by Government representatives or contractors designated by the Government. Site inspections will encompass inspections of information systems, operational, physical, and personnel security.

Security Decommissioning and Disposal

a) The Contractor must provide the Information Systems Decommissioning and Disposal Plan (ISDDP) (CDRL A0005). The contractor must update the ISDDP annually for the first 4 years following contract award, then every 2 years thereafter.

b) The Contractor must ensure that sensitive data, software, and hardware are protected from unauthorized disclosure, access, modification, or corruption as set forth in the approved Plan.

c) The Contractor must ensure that all sensitive data and information is unreadable for decommissioned hardware, software, and storage media in accordance with the approved Plan.

Security Reporting and Coordination

5.6.49.1 The Contractor must report (CDLR A0006) any evidence of security incidents within 15 minutes of the time of detection (e.g., unauthorized access of MEVA III services and detected security anomalies) to the NAS Cyber Operations (NCO) Group at 9-AJW-NCO@FAA.GOV or via phone at (540) 422-4114. The Contractor must also notify the FAA PMO within 24 hours of the incident.

5.7 SERVICE TESTING PROGRAM

The Contractor must conduct a testing program to ensure that MEVA III meets the performance requirements that are detailed in this contract. The principal goal of the

Service Testing Program is to verify that all the services provided under the contract meet the FAA's operational requirements**.**

Testing

5.7.2.1 The Contractor must establish a test program consistent with the following objectives:

a) The test program must be consistent with the Contractor's transition and implementation strategy.
b) The test program must provide verification of equipment installation, operational readiness, security, and network management functionality.
c) The test program must be consistent with the testing activities (Factor Acceptance Test (FAT) and Site Acceptance Test (SAT)) as described in the MEVA III RFP.

Contractor Conducted Test and Acceptance Activities

5.7.1.1 The Contractor must provide a comprehensive Test Plan (CDRL A0007) that describes in detail their plan for the conduct of test and acceptance of MEVA III services, including systems security. The plan must include a system verification requirements traceability matrix. All procedures and other documentation will be subject to FAA review and approval. The procedures used to implement the test methods must be industry-accepted techniques consistent with the evaluation and measurement of the requirement being verified.

5.7.1.2 The Contractor must notify the Program Office at least 5 working days prior to the start of any test activities. The FAA reserves the right to observe any and all of the test activities performed by the Contractor. The Contractor must provide FAA-designated personnel access to the Contractor's facilities for monitoring the set up and conduct of the test activities. When any service fails to meet a requirement, FAA acceptance will be withheld until the cause of the failure is identified and corrected. All test activities that fail must be repeated at no additional cost to the FAA until requirements are successfully met. The FAA reserves the right to increase the sample verification size for all failed services that need re-verification.

5.7.1.3 The Contractor must provide a Test and Evaluation report (CDRL A0008) containing the results of the contractor performed tests and evaluations, including security testing.

Independent Security Tests

5.7.4.1 The FAA, independent of other testing, will conduct Independent Security Tests in order to verify that the MEVA III network and services meet the MEVA III security requirements.

5.8 TRANSITION

The Contractor must interface with the FAA PM to plan, coordinate and conduct transition and cutover of all services from MEVA to MEVA III without interruption to critical aeronautical communications services. Transition must include but not be limited

to the process of planning, installing the infrastructure resources, transitioning circuits and activating services.

Transition Plan

5.8.1.1 The Contractor must provide a Transition Plan (CDRL A0009) that describes their approach to manage and implement MEVA III services as specified in this contract. The Plan must also address the approach to minimize disruption to FAA operations. The Transition Plan must be subject to FAA review and approval and take into consideration at least the following:

- Equipment Installation Testing
- Operational Readiness Testing
- Service Cutover Planning, Coordination and Scheduling
- Thirty Day System Performance Evaluation
- Service Acceptance Certification

5.9 Interoperability

The Contractor must provide all technical support, development, operations, procedures, software and equipment necessary to ensure any required interoperability between MEVA II and other Government telecommunications systems during transition to MEVA III.

The Contractor must maintain the current MEVA II Dialing Plan. The FAA will provide the Contractor with dialing numbers to be implemented.

5.10 Installation

The Contractor must provide all resources necessary to install all equipment, material and other resources to provide MEVA III service to the demarcation point.

Upon completion of installation and/or construction activities, the Contractor must be responsible for clean-up and disposal of any shipping crates, packing materials, and related items not required for MEVA III operation.

5.11 Regulatory Compliance

In the implementation of MEVA III services, the Contractor must be responsible for compliance with all applicable Federal, state and local environmental, safety and construction regulations. For installations at Government facilities, the Contractor must comply with the applicable documents listed in Section C Paragraph 2 Table 2-1.

5.12 Material

The Contractor must provide all material required for the installation and operation of equipment at Government facilities to provide MEVA III services. All material must be new. The Contractor must provide the following material, including but not limited to:

a) Racks, cabinets, and mounting hardware for MEVA III equipment,

b) All cabling from the facility cable entrance to the Government demarcation, unless otherwise provided by the FAA;
c) Power and ground cables, connectors, as necessary, to connect the MEVA III equipment to FAA-designated power supply panels and grounding buses;
d) Installation tools and test equipment;

5.13 Outside Equipment

If the Contractor requires space for a tower, earth station, or communication antenna, etc., the Contractor must coordinate with the Government for the location of these structures on a case-by-case basis. The Contractor must comply with all federal, state and local codes.

5.14 As Built Drawings and Manuals

The Contractor must provide, within 60 days following completion, testing and commissioning of a VSAT site installation, two sets of site as-built engineering records (CDRL A0010) to the FAA Program Office. The records must include a system block and level diagram, cable and circuit connection lists, power and grounding details, and all other details reflecting each installed site configuration.

In addition, the Contractor must provide two sets of the manufacturer's theory of operation and service manual for each item of new equipment supplied by the Contractor (CDRL A0011).

5.15 System Software

The Contractor must maintain the currency of all MEVA III software and firmware and notify the FAA in advance whenever software and firmware upgrades or changes are going to be implemented throughout the MEVA III Network.

Within 60 days after completion, testing, and commissioning of a VSAT site installation, the Contractor must provide the FAA with a copy of the site license for any commercial software used in the system.

5.16 System Cutover Support

The Contractor must support MEVA III cutover actions.

5.17 Moves and Changes

As ordered by the FAA via a task order, and as described in Section C 5.25, the Contractor must perform all actions required to move or change an existing service.

5.18 Discontinuation of Service

Upon service discontinuation, the Contractor must be responsible for the removal of all MEVA III equipment, material, and related items from FAA sites. The Contractor must be responsible for restoration of any disturbed earth.

The Contractor must be responsible for removal of hazardous materials associated with MEVA III equipment from FAA sites in accordance with applicable Federal, State and Local regulations.

5.19 Network Management Capability

The Contractor must provide a Network Management capability to manage the MEVA III network. The MEVA III network requires an integrated system that ties together, in a

single architecture, all MEVA III remote VSAT sites with the Network Control Computer and its supporting Network Management capabilities. The Contractor must use the Network Management capability to assess the performance and utilization of MEVA III services.

The Contractor must provide all hardware, software, and personnel required to meet the Network Management requirements specified in the MEVA III Request For Proposal (RFP).

The Contractor must maintain a computer based trouble ticket logging and reporting system for the MEVA III Network.

The Contractor must provide a primary and alternate Network Control Computer (NCC) for MEVA III that is in a physically secure facility with controlled access strictly limited to NCC operations staff and authorized visitors only.

5.20 Customer Support Service for Network Management

The Contractor must provide Customer Support Service that is accessible via toll-free phone access. The Contractor's Network Management Center (NMC) will be manned with English and Spanish-speaking operations staff 24 hours per day, 7 days a week, and 365 days a year.

The NMC staff must monitor the operational status and performance of the MEVA III network and assist in the process of trouble diagnosis and restoring service to satisfactory operational status in compliance with the requirements of the contract.

Customer Support Service Functions

5.20.1.1 The Contractor must provide the following Customer Support Service functions:

a) Provide technical assistance and support.
b) Accept reports of problems regarding MEVA III service and initiate the appropriate actions to resolve them.
c) The Trouble Ticket information produced in accordance with Section 4.9.3 of the contract must be updated every 60 minutes.

5.21 Record Keeping and Reporting

The contractor must maintain a log of all calls received by Customer Support Service in a database. As a minimum, the log must contain the following data elements for each call made to Customer Support Service: date and time call received, call pickup time, call waiting time, caller identification, the request, the action taken, result/response provided, service time, date and time the result/ response was provided, and the method used to provide the results (i.e. e-mail, fax, phone call, etc.). In addition, the Customer Support Service representative must log any other information necessary to document performance.

The contractor must deliver this log to the Government within 30 days after receipt of a written request by the Government. This reporting requirement only applies to the 2400 Customer Support Service number.

5.22 MEVA III Maintenance

The Contractor must provide a Maintenance Plan (CDRL A0012) which identifies the Contractor's maintenance organization(s) and describes the approach, processes, and procedures to be used to successfully maintain the system components that provide MEVA III services. The plan must address provisions for service continuity, service restoration, and routine and emergency maintenance at FAA sites. The plan must also address the approach to meeting the Service Level Agreement requirements of the contract.

The Contractor must provide all labor, supervision, materials, equipment, tools, and appliances to maintain and restore MEVA III services.

The Contractor must provide, maintain, repair and replace any new equipment required for the MEVA III network.

The Contractor must be responsible for performing all preventive and corrective maintenance for MEVA III services.

The Contractor must coordinate all maintenance activities with the Government prior to conducting maintenance at Government facilities. The Contractor must not proceed until the Government has released the affected services.

The contractor must provide and maintain all security related software patches, releases and upgrades, including but not limited to firewall, virus scanning and Intrusion Detection System rules/signatures, offered by manufacturers as an integral portion of their product support. This activity is considered a part of the preventive maintenance responsibility of the contractor and must be conducted as follows:

a. All signature and rule databases for computer virus scanning, intrusion detection and other similar security services must be updated within 24 hours after release of the update.
b. In response to specific security incidents or events, (internal and/or external to MEVA III) signature and rule databases for computer virus scanning, intrusion detection and other similar security services must be updated more frequently, as required (hourly or daily).

The Contractor must schedule preventive maintenance activities and must obtain concurrence from the Government at least 14 calendar days prior to performing any preventive maintenance activity that could adversely affect MEVA III services.

The Contractor must notify the Government prior to performing any corrective maintenance activity that could adversely affect MEVA III services. The Government reserves the right to delay or cancel any service interruption at any time prior to the commencement of preventive or corrective maintenance activity.

The Contractor must notify the FAA Program Office and site representatives at least 30 days in advance of scheduled service outages due to sun-transit outages.

The Contractor must notify the FAA site representative concerned fourteen (14) days in advance of schedule maintenance outages.

If the Contractor elects to use loop-back or responder devices, or other devices that utilize control signals for service monitoring or testing, usage must be coordinated with the

Government. After restoration and testing of any failed or jeopardized service, the contractor must obtain Government approval that the service is acceptable for use.

5.23 Contractor Initiated Changes

The Contractor must notify the FAA at least 60 calendar days in advance of any planned changes that could adversely affect MEVA III service, including but not limited to, hardware upgrades, software changes, firmware revisions, upgrades to the Network Management system and changes to improve performance or prevent future failures.

For all Contractor initiated changes, the FAA must have the right to require the Contractor to provide the reasons for the changes proposed and the schedule for implementation. Change notifications must be accompanied by sufficiently detailed engineering documentation and explanation. Any changes in the network or support systems made by the Contractor that result in service degradation/deficiencies, erroneous billing, or that impair interoperability within or among networks, must be rectified at no cost to the Government. In addition, the other provisions of this contract that pertain to service outages must apply.

The Contractor must obtain the approval from the FAA MEVA III Program Manager at least 30 days prior to performing any planned changes that would adversely affect FAA MEVA III services, including any periods of service outage for equipment maintenance or equipment/software changes.

5.24 MEVA III TRAINING

The Contractor must provide a Training Plan (CDRL A0013), which describes the Contractor's approach to familiarize FAA personnel with the services and features of MEVA III. The plan must address high-level (up to level 2) training, and on-site familiarization classes for new equipment installed at MEVA III sites.

The Contractor must conduct training based on the approved Training Plan.

5.25 Activation of New Services

The FAA may request new or additional equipment or aeronautical telecommunications services at any time during the term of the MEVA III contract via a Task Order. If engineering is required to satisfy the new service, the Service Provider must present a proposal and the associated cost for review and approval by the FAA. Engineering and technical support services may include, but are not limited to, network expansions, validation, and testing of interfaces to other electronic systems.

5.26 Miami Teleport Solution

The MEVA Member State FAA stated that the re-use of the existing antenna system in Miami is not possible any longer. Therefore, the FAA requested COMSOFT to prepare an alternative solution by the Teleport of COMSOFT's cooperation partner NEWCOM.

5.26.1.1 COMSOFT prepared the following solution to interconnect the uplink antenna on its Teleport Miami with the ACC of FAA

5.26.1.1.1 COMSOFT will use the existing C-Band antenna infrastructure, pointed to the satellite IS-14, which is required for the MEVA III VSAT network

5.26.1.1.2 IN addition, COMSOFT will provide rack space for the related VSAT equipment which will be shifted from FAA premises to the Teleport

5.26.1.1.3 The interconnection between the Teleport and FAA's ACC will be a redundant T1 interconnection line in order to keep the overall availability of the MEVA III network as requested by the Sealed Tender STe-22501390.

5.26.1.1.4 The most of the MEVA III equipment will be located at COMSOFT's Teleport, but there is additional equipment needed which has to be placed at FAA's premises (rack room) – multiplexer and redundancy switch.

5.26.1.1.5 To get a much better understanding of the solution, refer to the attached detailed network drawing of the MEVA III network site Miami.

5.26.1.1.6 The demarcation points are the voice / data interfaces at the RSS-16 switch.

5.26.1.1.7 See attached Equipment Provisioning List