CI-FSS-055 COMMERCIAL SATELLITE COMMUNICATION (COMSATCOM) SERVICES (DEC 2014)

To ensure the protection of controlled unclassified information (CUI) as required by Federal Information Security Management Act of 2002 and DoDM 5200.01-V4 (DoD Information Security Program: Controlled Unclassified Information (CUI) the following shall be implemented.

(a) *General Background.*

Special Item Numbers (SINs) have been established for Commercial Satellite Communications (COMSATCOM) services, focused on transponded capacity (SIN 132-54) and fixed and mobile subscription services (SIN 132-55), to make available common COMSATCOM services to all Ordering Activities.

(b) *Information Assurance.*

(1) The Contractor shall demonstrate, to the maximum extent practicable, the ability to meet:

(i) The Committee on National Security Systems Policy (CNSSP) 12, "National Information Assurance Policy for Space Systems used to Support National Security Missions," or

(ii) Department of Defense Directive (DoDI) 8581.1, "Information Assurance (IA) Policy for Space Systems Used by the Department of Defense."

(2) The Contractor shall demonstrate the ability to comply with the Federal Information Security Management Act of 2002 as implemented by Federal Information Processing Standards Publication 200 (FIPS 200), "Minimum Security Requirements for Federal Information and Information Systems." In response to Ordering Activity requirements, at a minimum, all services shall meet the requirements assigned against:

(i) A low-impact information system (per FIPS 200) that is described in the current revision of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems and Organizations,"

(3) The Contractor's information assurance boundary is where the Contractor's services connect to the user terminals/equipment (i.e., includes satellite command encryption (ground and space); systems used in the Satellite Operations Centers (SOCs), Network Operations Centers (NOCs) and teleport; and terrestrial infrastructure required for service delivery).

(c) *Delivery Schedule.*

The Contractor shall deliver COMSATCOM services in accordance with 552.211-78.

(d) *Portability*.

The Contractor shall have the capability to redeploy COMSATCOM services, subject to availability. Portability shall be provided within the COMSATCOM Contractor's resources at any time as requested by the Ordering Activity. When portability is exercised, evidence of equivalent net present value (NPV) shall be provided by the Contractor.

(e) *Flexibility/Optimization.*

The Contractor shall have the capability to re-groom resources for spectral, operational, or price efficiencies. Flexibility/optimization shall be provided within the COMSATCOM Contractor's resources at any time as requested by the Ordering Activity. When flexibility/optimization is exercised, evidence of equivalent net present value (NPV) shall be provided by the contractor. The Contractor is encouraged to submit re-grooming approaches for Ordering Activity consideration that may increase efficiencies for existing COMSATCOM services.

(f) *Net Ready* (Interoperability).

COMSATCOM services shall be consistent with commercial standards and practices. Services shall have the capability to access and/or interoperate with Government or other Commercial teleports/gateways and provide enterprise service access to or among networks or enclaves. Interfaces may be identified as interoperable on the basis of participation in a sponsored interoperability program.

(g) *Network Monitoring* (Net OPS).

The Contractor shall have the capability to electronically collect and deliver near real-time monitoring, fault/incident/outage reporting, and information access to ensure effective and efficient operations, performance, and availability, consistent with commercial practices. Consistent with the Contractor's standard management practices, the Net Ops information will be provided on a frequency (example: every 6 hours, daily) and format (example: SNMP, XML) as defined in a requirement to a location/entity/electronic interface defined by the Ordering Activity. Specific reporting requirements will be defined by the Ordering Activity.

(h) *EMI/RFI Identification, Characterization, and Geo-location.*

The Contractor shall have the capability to collect and electronically report in near real-time Electro Magnetic Interference (EMI) / Radio Frequency Interference (RFI) identification, characterization, and geo-location, including the ability to identify and characterize sub-carrier EMI/RFI being transmitted underneath an authorized carrier, and the ability to geo-locate the source of any and all EMI/RFI. The Contractor shall establish and use with the Ordering Activity a mutually agreed upon media and voice communications capability capable of protecting "Sensitive, but Unclassified" data.

(i) *Security.*

(1) The contractor may be required to obtain/possess varying levels of personnel and facility security clearances up to U.S. Government TOP SECRET/Sensitive Compartmented Information (TS/SCI) or equivalent clearances assigned by the National Security Authority of a NATO Member State or Major Non-NATO Ally.

(2) For incident resolution involving classified matters, the Contractor shall provide appropriately cleared staff who can affect COMSATCOM services operations (example: satellite payload operations, network operations). The Contractor shall provide a minimum of one operations staff member AND a minimum of one person with the authority to commit the company if resolution requires business impacting decisions (example: Chief Executive Officer, Chief Operations Officer, etc.).

(3) When Communications Security or Transmission Security equipment or keying material is placed in the equipment/terminal shelter, the Contractor shall ensure compliance with applicable physical security directives/guidelines and that all deployed equipment/terminal operations and maintenance personnel shall possess the appropriate clearances, equal to or higher than the classification level of the data being transmitted. Where local regulations require use of foreign personnel for terminal operations and maintenance, then the Contractor shall ensure compliance with applicable security directives/guidelines and document to the U.S. Government's satisfaction that protective measures are in place and such individuals have equivalent clearances granted by the local host nation.

(4) For classified operations security (OPSEC), the Contractor shall ensure that all personnel in direct contact with classified OPSEC indicators (example: the unit, location, and time of operations) have U.S. SECRET or higher personnel security clearances, or, as appropriate, equivalent clearances assigned by the National Security Authority of a NATO Member State or Major Non-NATO Ally, in accordance with applicable security directives and guidelines.

(5) To ensure the capability of communicating classified intelligence information to satellite vendors cleared satellite vendor/staff must have access to secure voice communications for emergency purposes. Communications security equipment (COMSEC) certified by the National Security Agency (NSA) to secure critical unclassified and up to and including SECRET communication transmissions at their operating locations is required.

(6) The Contractor shall have the capability to “mask” or “protect” users against unauthorized release of identifying information to any entity that could compromise operations security. Identifying information includes but is not limited to personal user and/or unit information including tail numbers, unit names, unit numbers, individual names, individual contact numbers, street addresses, etc.

(j) *Third party billing for COMSATCOM subscription services.*

The Contractor shall identify authorized network infrastructure for the Ordering Activity. In some cases, the user of the terminal may access network infrastructure owned or operated by a third party. In the event a terminal is used on a third party’s network infrastructure, the Contractor shall provide to the Ordering Activity, invoices and documentation reflecting actual usage amount and third party charges incurred. The Ordering Activity shall be billed the actual third party charges incurred, or the contract third party billing price, whichever is less.

(k) *DoD Solicitation Pre and Post Award Requirement for Communications and Data Protection Using External Certificate Authority Public Key Infrastructure (ECA PKI).*

To ensure the protection of controlled unclassified information (CUI) as required by Federal Information Security Management Act of 2002 and DoDM 5200.01-V4 (DoD Information Security Program: Controlled Unclassified Information (CUI) the following shall be implemented.

(1) Vendors shall digitally sign and encrypt all DoD RFQ and task order related documents, to include contract deliverables, emailed to government agents. Government agents include, but are not limited to, DISA (COMSATCOM Center), DITCO, the Regional SATCOM Support Centers, General Services Administration, users of contractor-provided services, and government-contracted support. Digital signatures and encryption shall be provided through the use of Medium Hardware Assurance Public Key Infrastructures certificates, and associated hardware, issued by one of the approved External Certificate Authority (ECA) vendors. Contractors that desire to respond to DoD task order solicitations, receive and perform DoD task orders shall obtain this capability within 10 days after award of Schedule 70 Contract SINs 135-54 & 132-55 or BPAs for satellite services. Existing Schedule 70 Contractor holders of SINs 132-54 & 132-55 interested in bidding on DoD Task Orders shall obtain this capability prior to bidding on any DoD solicitations.

(2) The following DISA web page (http://iase.disa.mil/pki/eca/) provides links to approved ECAs. To obtain a certificate, select one of the approved ECA vendors and complete the registration. Each individual registering for a PKI certificate must verify their identity during the registration process. ECA vendors charge a fee for each registration.