SECTION C
DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

C.1 OVERVIEW

C.1.1 CONTRACT OBJECTIVE

C.1.1.1 The overarching objective for Complex Commercial SATCOM Solutions (CS3) is to create contracts as flexible and agile as possible to meet and satisfy the widely differing requirements of the Federal Government organizations both now and for the next decade and beyond. CS3 is intended to meet program goals for:

- Service Continuity
- Highly Competitive Prices
- High-Quality Service
- Full Service Vendors
- Operations Support
- Transition Assistance and Support
- Opportunities for Technical Innovation

C.1.1.2 Contractors are sought who will provide worldwide commercial satellite communications (COMSATCOM) Complex Solutions. COMSATCOM Complex Solutions comprise customized engineered solutions to meet customers' unique COMSATCOM needs. These solutions may include any combination of fixed satellite services and/or mobile satellite services, components, and/or service enabling authorizations (e.g., host nation approvals, landing rights, frequency clearances, etc.) and components and ancillary equipment such as terminals, teleports, terrestrial tail circuits, Subscriber Identity Module (SIM) cards, and peripherals.

C.1.1.3 COMSATCOM Complex Solutions may include, but are not limited to, design, development, licensing, integration, installation, testing, network management, engineering, full lifecycle logistics and operations support, and training. Delivered solutions may be turnkey systems comprising all elements of a system, or delivered solutions may be limited to integration of specific components with existing Government-provided elements. Examples of the types of COMSATCOM Complex Solutions the Contractor shall have the capability to deliver are included in this section; however, the specific COMSATCOM Complex Solutions to be procured will be defined in subsequent Task Orders.

C.1.2 EMERGING TECHNOLOGY AND SECURITY

The Government recognizes that satellite technologies and services are rapidly evolving. Accordingly, the Government anticipates that services and solutions available under CS3 will be increased, enhanced, and upgraded as these improvements become available to COMSATCOM customers. It is anticipated that over the life of the CS3 contracts, the current information assurance policies and procedures for COMSATCOM Complex Solutions will continue to evolve to address system vulnerabilities and cyber-threats.

C.2 SUMMARY OF REQUIREMENTS

Unless otherwise instructed in this Contract, the Contractor is solely responsible for all requirements stated herein.

C.2.1 MANAGEMENT REQUIREMENTS

C.2.1.1 Program Management

C.2.1.1.1 The Contractor shall employ project management processes and resources needed to plan, direct, coordinate, and implement the contract as well as control the requirements contained in the contract and priced Task Orders. The Contractor shall have the capability to manage multiple simultaneous Task Orders of varying complexity at worldwide locations, including:

- Methodologies and tools for planning the activities of its team(s)
- Scheduling, organizing, and deploying resources
- Controlling task execution, monitoring progress, and resolving critical issues

C.2.1.1.2 The Contractor shall furnish effective and proactive management of the full Task Order lifecycle for COMSATCOM Complex Solution to include award, Task Order kickoff, transition and onboarding, design, procurement, development and staging, fielding, testing and integration, system acceptance, on-going maintenance and operational support. The Contractor shall manage and minimize Task Order risks at all subcontract tiers.

C.2.1.1.3 The Contractor shall implement and maintain a governance and reporting structure that provides transparency and Government access to cost, schedule, and performance metrics, and supports timely delivery of services and accurate invoicing.

C.2.1.1.4 The Contractor shall manage resources as required throughout the Task Order lifecycle to include staff recruitment, training and evaluation of performance. The Contractor shall have the capability to manage resources when there are reductions or surge in Task Order workload, and when there are requirement changes necessitating reallocation of resources.

C.2.1.1.5 The Contractor shall document work to be allocated to Subcontractors and the processes for managing Subcontractors. The Contractor shall employ metrics that will be utilized with the Government and with Subcontractors to provide effective management of Task Order performance.

C.2.1.1.6 On a Task Order basis, the Contractor shall provide resumes for personnel contributing to a COMSATCOM Complex Solution as requested to address specific personnel requirements.

C.2.1.2 System Engineering

C.2.1.2.1 The Contractor shall develop and document an engineered solution that addresses all requirements as outlined in this contract and the specific Task Order.

C.2.1.2.2 The Contractor shall develop and document an engineered solution that identifies all equipment and resources proposed to satisfy the Task Order.

C.2.1.2.3 The Contractor shall develop and document an engineered solution that provides the Contractor recommended plans to replace equipment and resources in case of failure, except in those cases where the Government has specific sparing requirements.

C.2.1.2.4 The Contractor shall develop and document an engineered solution that addresses the use of Government furnished materials and resources as specified in the Task Order.

C.2.1.2.5 The Contractor shall develop and document an engineered solution that implements the necessary quality processes and quality control. The Contractor shall provide the necessary infrastructure and practices to ensure service availability requirements identified in the Task Order.

C.2.1.2.6 The Contractor shall develop and document an engineered solution that effectively identifies and assesses risk. The Contractor shall document and implement a risk management strategy for the Task Order.

C.2.1.2.7 The Contractor shall update the engineered solution to reflect all Task Order modifications and incorporate Engineering Change Proposals (ECPs) as required.

C.2.1.2.8 The Contractor shall ensure any Network Operations Center (NOC) identified as part of the engineered solution has the following minimum functional capabilities[1]:

- Spectrum and Network Monitoring
- Incident Response
- Automated Reporting

C.2.1.2.9 The Contractor shall develop and document an engineered solution that identifies the applicable performance standards, specifies the set of performance metrics for the services the Contractor proposes to use, and describes in detail the methods and measurements with which the Contractor proposes to establish compliance with the performance standards. The Government reserves the right, on a Task Order basis, to identify the performance standards, specify the performance metrics, and describe the methods and measurements to establish compliance with the performance standards.

C.2.1.3 Information Security and Risk

The Contractor shall ensure effective implementation and management of an information security program to provide security for all systems, networks, and data that support the operations of the organization. Additionally, the Contractor shall ensure that all COMSATCOM Complex Solutions provided are compliant with information assurance requirements.

C.2.1.4 Risk Management Framework

The National Institute of Standards and Technology (NIST) working with the Department of Defense and other organizations developed a common information security framework for the Federal Government and its contractors. The Risk Management Framework (RMF) replaces the traditional certification and accreditation (C&A) process and includes a continuous monitoring process. The RMF steps[2] include:

[1] Additional Functional Capabilities may be identified in the Task Order
[2] National Institute of Standards and Technology Special Publication 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, Section 1.1 and Section 2.1

Categorize the information system and the information processed, stored, and transmitted by that system based on an impact analysis.

Select an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.

Implement the security controls and describe how the controls are employed within the information system and its environment of operation.

Assess the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Authorize information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.

Monitor the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

The Contractor will develop a Risk Management Framework Plan that includes processes and procedures to accomplish all of the above steps except Authorize[3]. The Authorize step will be completed for each Task Order by the Ordering Activity. The Risk Management Framework Plan will be a post-award contract deliverable (see Section F.6).

C.2.1.5 Climate Change Risk and Mitigation

GSA has a leading role in ensuring that the Federal Government is better prepared to cope with the consequences of climate change that present many serious risks for government operations. These risks include damage to facilities and equipment and disruptions to communications networks. Climate change risk and mitigation shall be considered in the design and operations of services to be provided under this contract.

The Contractor shall incorporate climate change adaptation strategies into risk-management programs to reduce property, infrastructure, and supply chain vulnerabilities. This includes identifying mission critical facilities, products and services, evaluating business operations and supply chains that may be vulnerable and anticipating needs that may arise from climate change.

[3] NIST 800-37 Security Authorization is the official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizations operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

Executive Order (E.O.) 13693, *Planning for Federal Sustainability in the Next Decade*, requires agencies to identify and address projected impacts of climate change on mission critical communication demands and consider those impacts in operational preparedness planning. In support of this requirement, contract awardees shall prepare and update as needed a Corporate Climate Risk Management Plan that identifies, and addresses mitigation of, climate change risks to land based equipment and services associated with the satellite communication services provided under this contract. The Corporate Climate Risk Management Plan will be a post-award contract deliverable (see Section F.6).

C.2.1.6 Cost and Schedule

The Contractor shall provide customers with accurate schedules and project status, timely and accurate invoicing, and provide account information as defined in subsequent Task Orders to the Ordering Contracting Officer (OCO), Contracting Officer's Representative (COR), and Task Leads.

C.2.2 GENERAL TECHNICAL REQUIREMENTS

C.2.2.1 The Contractor shall provide complete, customized engineered COMSATCOM Complex Solutions to meet customers' unique satellite communications needs. These solutions may include any combination of fixed satellite services or mobile satellite services components, and/or service enabling components such as terminals, teleports (to include both Gateway and Telemetry, Tracking, and Control (TT&C) systems), Network Operations Centers (NOC), and terrestrial interface tail circuits. The Contractor shall also have the ability to supply licensing, integration, network management, engineering services, and any necessary ancillary equipment and services.

C.2.2.2 The Contractor shall provide the COMSATCOM system engineering design, configuration, installation, implementation, training, and on-going maintenance and operational support necessary to deliver a COMSATCOM Complex Solution. The Contractor shall design solutions that allow for purchase of solution components (where the Government retains ownership of equipment, e.g. satellite transponder) and/or leasing of solution components (where the Contractor retains ownership of equipment). The Contractor shall have the ability to provide a solution-specific combination of at least, but not limited to, the services identified below:

> **C.2.2.2.1** Design and Engineering Services including, but not limited to, site surveys, developing specifications, drawings, reports, schedules and other related work products, configuration, procurement, implementation, installation and testing.

C.2.2.2.2 Ongoing Maintenance and Operational Support Services including, but not limited to, network management, operations support, gateway operations, full lifecycle logistics support, quality assurance, asset management, maintenance and repair services.

C.2.2.2.3 Customer Care and Helpdesk Support including, but not limited to, facilitating satellite and network access, responding to trouble calls and complaints with identified points of contact, availability, and procedures for problem resolution, information flow, and escalation. Personnel providing Customer Care and Helpdesk Support must be English-speaking. The individual customer requirements will define the methods of customer access and hours of operation up to 24 hours per day, 7 days a week.

C.2.2.2.4 Training shall include, but is not limited to: satellite access procedures, equipment operations, and maintenance training.

C.2.3 REQUIRED COMSATCOM COMPLEX SOLUTION TYPES

C.2.3.1 COMSATCOM Complex Solutions include, but are not limited to, any combination of bandwidth, throughput, terminals, other user equipment, teleports, terrestrial tail circuits, networks, other terrestrial infrastructure, integration and engineering services, and installation, operations, and maintenance.

C.2.3.2 The Contractor solutions shall meet the Information Assurance, Responsiveness, Portability, Flexibility/Optimization, Capacity, Coverage, Net Ready (Interoperability), Network Monitoring (Net Ops), Electro Magnetic Interference (EMI) / Radio Frequency Interference (RFI) Identification, Characterization, and Geo-location, and Security requirements outlined in Section C.2.4 as assigned by the Ordering Activity on a Task Order basis.

C.2.3.3 The Contractor shall have the capability to deploy the necessary terminals, teleports, terrestrial tail circuits, networks, Integration Services, Engineering Services, Licensing, Network Management, Operations & Maintenance, and Training required by the Ordering Activity. The Contractor must provide documentation required to conduct Security Assessments and obtain a Security Authorization.[4]

C.2.3.4 The Contractor shall provide the necessary capabilities and deliver solutions of the scope herein, in response to requirements aligning with the COMSATCOM Complex Solution types described in C.2.3.4.1 through C.2.3.4.9. Additionally, content/solution types/applications (e.g., broadcast technology) that is connected to a satellite network may be considered in-scope if the majority of the solution is satellite-orientated.

[4] See footnote 2.

C.2.3.4.1. Interactive Services. The Contractor shall have the capability to provide complete, customized engineering solutions to support 24x7 Interactive Services requirements. Interactive Services involve the ability to connect multiple locations into a real-time two-way interactive network, mostly involving audio and video. Interactive Services include Distance Learning and Telemedicine type requirements. Interactive Services are often characterized by distribution of a common information stream to multiple locations, scheduling components, and conditional access management. Interactive Services must allow for changes to the information stream, distribution locations, and network configurations. Interactive Services must also accommodate changing circumstances and variances with terrestrial communication components and systems, to address the level of customer tolerance for latency, delay, jitter, and packet loss.

C.2.3.4.2 Continuity of Operations (COOP). The Contractor shall have the capability to provide complete, customized engineering solutions to support COOP requirements. COOP involves the pre-planned establishment and deployment of a backup or alternative communications infrastructure in anticipation that a natural or human-caused event disables or destroys the normal, primary communications infrastructure and is focused on reconstitution of the critical communications functionality to continue minimal essential and/or normal operations. When the COOP capability is required, activation is often required within 24 hours. COOP includes developing an alternative for portions of, or the entirety of, the normal, primary communications infrastructure, and can be

as simple as a set of new Internet Protocol addresses or as complex as replicating the functionality of the entire primary, terrestrial infrastructure. COOP can include requiring a completely different set of hardware, personnel, and network paths, and associated terrestrial infrastructure as an ancillary component of the COMSATCOM Complex Solution.

C.2.3.4.3 Broadcast Satellite Service (BSS). The Contractor shall have the capability to provide complete, customized engineering solutions to support BSS requirements. BSS involves the collection of voice, video, and/or data into one central site and subsequent distribution of that information (typically one-way) to multiple fixed and/or mobile locations. BSS includes Streaming Media type requirements. BSS is often characterized by high bandwidth requirements, dedicated, fully utilized data streams for the duration of the broadcast, live or real-time distribution, access control for different portions of the information stream, and minimum customer tolerance for latency, delay, and jitter.

C.2.3.4.4 Fleet and Asset Tracking & Reporting Services. The Contractor shall have the capability to provide complete, customized engineering solutions to support Fleet and Asset Tracking & Reporting Services requirements. Fleet and Asset Tracking & Reporting Services involve the ability for deployed equipment (e.g., sensors) to send real-time location and/or status information or the ability to send messages or other data to the fleet. Fleet and Asset Tracking & Reporting Services include machine-to-machine (M2M) technologies and data transfer.

C.2.3.4.5 Emergency Responder Operations. The Contractor shall have the capability to provide complete, customized engineering solutions to support Emergency Responder Operations. Emergency Responder Operations involve reconstituting a communications infrastructure in response to a natural or human-caused event that disrupts or destroys the normal, pre-existing communications infrastructure. Emergency Responder Operations involves an ad-hoc, immediate need communications requirement that eventually reverts back to communications infrastructure previously used or restored. Emergency Responder Operations needs quick responsiveness from a few hours to a few days, and optimally provides interoperability among different types of responders, transportability, quick design, implementation, and activation, and the ability to reach back into headquarters and shared information sources. Additionally, it is not uncommon for the requirement to grow significantly from a small number of users (e.g., initial responders) to a large number (e.g., coordinated large-scale humanitarian effort) within a moderate period of time (e.g., within 30 days).

C.2.3.4.6 Steady State Operations. The Contractor shall have the capability to provide complete, customized engineering solutions to support Steady State Operations requirements which are generally long duration baseline communications services and infrastructure to support enduring user requirements. Steady State Operations include significant pre-planning with more time allowed for design, configuration, implementation, and activation times, ubiquitous access to collaborative and integrated users, fixed infrastructure that responds more slowly to changes, lower priority with the ability to be pre-empted by a higher priority (e.g. Emergency Responder Operations or Direct Customer Operations) short term need for the same communications resources. Steady State Operations generally has high sensitivity to the cost of the technical capability delivered.

C.2.3.4.7 Direct Customer Operations. The Contractor shall have the capability to provide complete, customized engineering solutions to support Direct Customer Operations requirements which are typically of short duration to support a specific mission. Direct Customer Operations involve the creation of a communications infrastructure to support specific Customer operations, usually because no pre-existing communications infrastructure is available. Direct Customer Operations include the ability to collaborate among various types of Customers and connect Customers operating on the tactical edge back to headquarters and shared information sources. Direct Customer Operations often require transportability and mobility, personnel and facility security, information assurance, and the ability to reconfigure and/or reconstitute quickly in response to changing situations during prosecution of the mission with real-time insight into communications networks status, and moderate to quick responsiveness requirements with deployment required in several hours to several days. These communications solutions can be high priority with the ability to pre-empt other uses of the same communications resources, and typically the cost of the solution is a much lower priority than the ability to utilize the solution as part of executing the mission. Additionally, the requirement may grow significantly from a small number of users (e.g., 50 users or less) to a much larger number within a moderate period of time (e.g., within 30 days).

C.2.3.4.8 Stand-alone Satellite Professional Support Services. [APPLICABLE FOR SMALL BUSINESS CONCERNS ONLY]. The Contractor shall provide COMSATCOM-related Professional Support Services for all COMSATCOM Complex Solution components to include any or all support services. These services include, but are not limited to, abstract or concept studies and analysis, strategic and preliminary planning, requirements definition and analysis, evaluation of alternative technical approaches, modeling and simulation, enterprise architecture design, cost-performance trade-off analysis, feasibility analysis, regulatory compliance support, system engineering, independent verification and validation, network performance assessment, and, and Information Assurance Security Assessment and Security Authorization.

C.2.3.4.9 The Government reserves the right to issue requirements aligned with COMSATCOM Complex Solution types not included in the list above.

C.2.4 REQUIRED COMSATCOM COMPLEX SOLUTION ATTRIBUTES

Required COMSATCOM Complex Attributes are common attributes that apply to all COMSATCOM Complex solution types. These attributes are in line with the COMSATCOM attributes that were validated by the DoD Joint Staff Net-Centric Functional Capabilities Board (NC FCB) Memorandum, "The Net-Centric Assessment of Commercial Satellite Capabilities," dated 21 February 2006."

C.2.4.1 Information Assurance

C.2.4.1.1 The Contractor shall comply with: The Committee on National Security Systems Policy (CNSSP) 12, "National Information Assurance Policy for Space Systems used to Support National Security Missions," or Department of Defense Instruction (DoDI) 8581.01, "Information Assurance (IA) Policy for Space Systems Used by the Department of Defense."

C.2.4.1.2 The Contractor shall 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." All Contractor solutions will be evaluated against a moderate-impact information system (per FIPS 200) that is described in the current revisions of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," NIST SP 800-37 "Guide for Applying the Risk
Management Framework to Federal Information Systems", DoD Instruction (DoDI) 8500.01, "Cybersecurity," DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)" and associated documents.

C.2.4.1.3 On a Task Order basis, the Ordering Activity shall assign an impact level (Low, Moderate, or High, per FIPS 200, NIST SP 800-53, DoDI 8500.01 and DoDI 8510.01) prior to issuing the initial statement of work. Task Order evaluations shall consider the extent to which the Contractor solutions complies with the necessary security controls based upon the assigned impact level, command encryption/authentication, and other requirements in CNSSP 12 and/or DoDI 8581.1.

C.2.4.1.4 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), Business Support Systems (BSS), and teleport; and terrestrial infrastructure required for service delivery). On a Task Order basis, the Ordering Activity shall define the IA boundary in their Statement of Work or Performance Work Statement (PWS).

C.2.4.1.5 The Ordering Activity reserves the right to independently evaluate, audit, and verify the IA compliance for any proposed or awarded COMSATCOM Complex Solution. The Contractor must provide documentation required to conduct Security Assessments and Security Authorization. All IA Security Assessments and Security Authorizations are the responsibility of the Ordering Activity.

C.2.4.2 Responsiveness

C.2.4.2.1 As specified on a Task Order basis, the Contractor shall deliver solutions in one of the following timeframes after Task Order award:

C.2.4.2.1.1 Standard Service Delivery (30 calendar days or less). Standard Service Delivery is the time required under normal conditions for COMSATCOM Complex Solutions to be available.

C.2.4.2.1.2 Accelerated Service Delivery (7 calendar days or less). Under Accelerated Service Task Orders, service acceptance testing unless otherwise required by the satellite provider or host nation shall be deferred until operations permit.

C.2.4.2.1.3 Time-Critical Service Delivery (4 hours or less). Under Time-Critical Service Task Orders, service acceptance testing unless otherwise required by the satellite provider or host nation shall be deferred until operations permit. Time-Critical Delivery shall be predicated on the availability of pre-planned engineering solutions, pre-planned line-up messages and transmission plans, pre-arranged Host Nation Agreements (HNA), terrestrial connectivity (if applicable), and frequency clearance, and the availability of contracted bandwidth.

C.2.4.2.1.4 Extended Service Delivery. The time required under extenuating circumstances to implement a Task Order after order award. Such extenuating circumstances may include extended time required for host nation agreements or landing rights, long-lead terrestrial connectivity,

or other time intensive service delivery requirements as defined in the individual Task Order. Any such extended delivery times will be negotiated between the Ordering Activity and Contractor.

C.2.4.3 Portability

C.2.4.3.1 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 and is not limited to the examples provided below. When portability is exercised, evidence of equivalent net present value (NPV[5]) shall be provided by the Contractor. Alternatively, prior to Task Order award, specific pre-defined terms and conditions for portability and related services including pricing and/or other contract terms may be negotiated and defined in the individual Task Order.

C.2.4.3.2 Portability may include moving from one transponder/satellite to another, one managed service area to another, transponded capacity redeployment between beams or transponders on a single satellite, redeployment from one frequency band to another, physical relocation of a satellite to a new orbital position, re-routing of teleport services from one teleport to another pre-defined teleport, re-routing of traffic from one terrestrial infrastructure to another pre-defined infrastructure, and movement of Network Operations Center (NOC) services from one NOC to another NOC.

C.2.4.3.3 Any changes to the network architecture as a result of portability will require the Contractor to provide updated documentation to obtain approval / review of the security authorization with the Ordering Activity.

C.2.4.4 Flexibility/Optimization

C.2.4.4.1 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[6]) shall be provided by the Contractor. The Contractor is encouraged to submit re-grooming

[5] For example, one-year of service for a transponder valued at $1M/year is traded for six-months of service on a transponder valued at $2M/year.
[6] For example, one-year of service on a less efficient arrangement of contractor resources is traded for nine-months of services on a more efficient arrangement of contractor resources that provides an operational efficiency to the Ordering Activity's customers.

approaches for Ordering Activity consideration that may increase efficiencies for existing COMSATCOM Complex Solutions. Alternatively, prior to Task Order award, specific pre-defined terms and conditions for re-grooming including pricing and/or other contract terms may be negotiated and defined in the individual Task Order.

C.2.4.4.2 Re-grooming may include, but is not limited to, analysis of space segment, teleport, and network resource utilization in order to increase the number of carriers on existing allocated bandwidth and/or terminals and/or increasing the data rates on individual Task Orders through the implementation of advanced coding, modulation, and/or hardware upgrades.

C.2.4.4.3 Any changes to the network architecture as a result of regrooming will require the Contractor to provide updated documentation to obtain approval / review of the security authorization with the Ordering Activity.

C.2.4.5 Capacity

C.2.4.5.1 The Government has requirements for scalable COMSATCOM capacity in any COMSATCOM frequency band. The Contractor must be able to provide scalable capacity in any available COMSATCOM frequency band in support of US Government COMSATCOM requirements. The Contractor must be able to demonstrate
how they will provide surge capacity to the US Government when required at the individual Task Order level.

C.2.4.5.2 Any changes to the network architecture to provide surge capability will require the Contractor to provide updated documentation to obtain approval / review of the security authorization with the Ordering Activity.

C.2.4.6 Coverage

C.2.4.6.1 The Government has requirements for COMSATCOM coverage anywhere in the world and in any COMSATCOM frequency band. The Contractor must be able to provide coverage anywhere worldwide in any available COMSATCOM frequency band. Specific pre-defined coverage may be negotiated and defined in the individual Task Order.

C.2.4.7 Network Monitoring (Net Ops)

C.2.4.7.1 The Contractor shall have the capability to electronically collect and deliver near real-time spectrum and network 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 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. Prior to Task Order award, specific pre-defined terms and conditions for Net Ops collection and delivery may be negotiated and defined in the individual Task Order.

C.2.4.8 EMI/RFI Identification, Characterization, and Geo-Location

C.2.4.8.1 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. The Contractor shall provide best-effort capability to identify and characterize sub-carrier EMI/RFI being transmitted underneath an authorized carrier, and 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 Controlled Unclassified Information (CUI).

C.2.4.9 Security

C.2.4.9.1 To ensure the capability to respond to Secret national security requirements as identified in C.2.4.9.3 – C.2.4.9.6, the CS3 Contract is requiring contractors to obtain a Secret Facility Clearance with Secret level Safeguarding, and COMSEC requirements. The DD Form 254 (Contract Security Classification Specification) reflects these requirements and is attached (see sample Contract DD Form 254 in Section J). The GSA will issue a DD Form 254 upon contract award.

C.2.4.9.2 Task orders may require and identify higher level Facility, Safeguarding, special access, and COMSEC requirements. These requirements will be identified on the agency-specific DD Form 254 to be awarded at the Task Order level. A blank DD Form 254 is available at the following site: www.dtic.mil/whs/directives/forms/eforms/dd0254.pdf

C.2.4.9.3 The Contractor is responsible for providing personnel with appropriate security clearances to ensure compliance with government security regulations, as specified within the CS3 DD 254 and Task Orders. The Contractor shall fully cooperate on all security checks and investigations by furnishing requested information to verify the Contractor employee's trustworthiness and suitability for the position. Clearances

may include Sensitive Compartmented Information (SCI), Special Access Programs (SAP), or agency-specific access, such as a Q.

C.2.4.9.4 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 North Atlantic Treaty Organization (NATO) Member State or Major Non-NATO Ally.

C.2.4.9.5 The Contractor may be required to provide physical security (e.g., personnel or equipment protection).

C.2.4.9.6 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.).

C.2.4.9.7 When Communications Security (COMSEC) or Transmission Security (TRANSEC) 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.

C.2.4.9.8 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.

C.2.4.9.9 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 (COMSEC) equipment certified by the National Security Agency (NSA) to secure critical unclassified information (CUI) and up to and including SECRET communication transmissions at all operations centers is required.

C.2.4.9.10 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.

C.2.4.10 Net Ready (Interoperability)

The Contractor shall deliver solutions that are consistent with commercial standards and practices. Contractor solutions 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. Any such access and/or interoperability with teleports/gateways and provisioning of enterprise service access will be defined in the individual Task Order requirements.

(END OF SECTION C)