



ATTACHMENT J-15 DD FORM 254 TEMPLATE CONTINUATION PAGES

Prime Contract Number: GS00Q17NRD4003
Contractor (By Light Professional IT Services, Inc.)

10k(1). IAW DoD 5200.2-R, Personnel Security Program (current edition: January 1987, through Change 3, February 23, 1996), Contractor positions established in support of the Complex Commercial SATCOM Solutions (CS3) contract are assigned to one of two sensitivity designations Automated Data Processing II (ADP-II), Non-critical-Sensitive Positions or ADP-III, Non-sensitive Positions. The Contractor will ensure that individuals assigned to each sensitivity designation, as determined by the Government, have completed the appropriate forms and investigations. Necessary security clearances will be based on Defense Security Service (DSS) checks.

Required investigations will be completed prior to the assignment of individuals to sensitive duties associated with the position. The Contractor will forward employee clearance information to Defense Information System Agency (DISA) Industrial Security (MPS6).

DISA retains the right to request removal of Contractor personnel, regardless of prior clearance or adjudication status, whose action, while assigned to activities associated with this contract, clearly conflict with the interests of the Government. The reason or removal will be fully documented in writing by the Contracting Officer. When and if such removal occurs, the Contractor will within 30 working days assign qualified personnel to any vacancies thus created.

DoD 5200.2-R provided under separate cover.

11c: Contractor will reference the appropriate security classification guidance when generating or deriving classified material or hardware. All classified information received or generated will be properly stored and handled according to the markings on the material. All classified information received or generated is the property of the U.S. Government. At the termination or expiration of this contract, the U.S. Government will be contacted for proper disposition instructions. Contractor will abide by the following security classification guidance:

- DISA Circular 300-110-3, "Defense Information System Network (DISN) Security Classification Guide" [current edition dated August 14, 2008]. DISA Circular 300-110-3 provided under separate cover.
- DoDM 5200.01 Volume 1, Security Program Overview; Volume 2, Marking of Classified; and Volume 3, Protection of



Classified. DoDM 5200.01 Volumes 1, 2 and 3 will be provided under separate cover.

11d: The Contractor is required to store Communications Security (COMSEC) equipment (i.e., STEs), and associated keying material (i.e., Fortezza cards), classified document hardcopies, classified document softcopies and is required to have the following requirement(s): not less than an GSA-approved, 2 drawer, 2 cubic feet safe for storage of classified material.

11f: Contractor and its Subcontractors, when traveling or performing work outside the United States, Puerto Rico, and U.S. Possessions and Trust Territories under this contract shall:

- i. Affiliate with the Overseas Security Advisory Council, if the Contractor or Subcontractor is a U.S. entity;
- ii. Ensure personnel who are in-country on a non-transitory basis, register with the U.S. Embassy, and that Contractor or Subcontractor personnel who are third country nationals comply with any security related requirements of the Embassy of their nationality;
- iii. Provide personnel with antiterrorism/force protection awareness information commensurate with that the DoD provides to its military and civilian personnel, to the extent such information can be made available prior to travel outside the U.S.;
- iv. Obtain and comply with the most current antiterrorism/force protection guidance for Contractor personnel;
- v. Restrict performance of classified work to the sites indicated in the individual task orders.

11g: Technical information on file at the Defense Technical Information Center (DTIC) will be made available to the Contractor if the Contractor requires such information.

11h: The requirements and procedures for the protection of COMSEC information are set forth in the National Industrial Security Program Operating Manual (NISPOM) [current edition: DoD 5220.22-M dated February 28, 2006, Incorporating Change 1, March 28, 2013]. The COMSEC requirements of the NISPOM are imposed on the Contractor for safeguarding the COMSEC information. Contractor is authorized to receive Government furnished cryptographic equipment. Access to any classified COMSEC information requires special briefings at the Contractor's facilities. Access to classified COMSEC information requires a final U.S. Government clearance at the appropriate level. Non-accountable COMSEC information, though not tracked in



the COMSEC material control system, may still require a level of control within a document control system; refer to NSA/CSS Manual 3-16, Control of Communications Security Material, page E-4 for guidance. Methods of destruction of classified COMSEC material shall comply with the NISPOM (Ref: Section 5-705 of DoD 5220.22-M). Further disclosure of COMSEC information by a Contractor, to include subcontracting, requires prior approval of the Government contracting activity. DoD 5220.22-M and NSA/CSS Manual 3-16 provided under separate cover.

11i: The Contractor shall not process classified information by electrical means prior to a DISA TEMPEST evaluation of the equipment/systems and facility, and written DISA certification that the facility meets DISA TEMPEST criteria. In order to expedite the DISA TEMPEST evaluation, the Contractor shall provide a list of equipment, to include model number, which is associated with the processing of classified information. In addition, the estimated percentage of classified information processed, cable/conduit runs, a floor plan layout that depicts placement of equipment in relation to other rooms, equipment distances from walls or uncontrolled areas, and physical security being afforded the equipment both during processing and after hours. The above TEMPEST evaluation and DISA approval will not be required if previous DISA approval can be furnished and is no more than 2 years old. The existing approval must be for processing information at the same or higher level and at the same facility and items of equipment. The DISA Certified TEMPEST Technical Authority is the only authorized approving agent for TEMPEST systems within DISA.

11j: The Contractor will comply with Operations Security (OPSEC) requirements contained in the contract, NISPOM (Ref: DoD 5220.22-M), and the Industry Security Regulation (Ref: DoD 5220.22-R, Chapter 10, *Operations Security (OPSEC)*). Contractual OPSEC requirements above those contained within NISPOM shall be included in the appropriate requisition documentation (e.g., Task Order (TO) Request for Proposal) and resultant contract addendum (e.g., TO Order in sufficient detail to ensure complete Contractor understanding of exactly what special OPSEC provisions are required. DoD 5220.22-R provided under separate cover.

11k: Contractor authorization to use the Defense Courier Service will be obtained IAW DoDI 5200.33, "Defense Courier Operations" [Current edition: June 30, 2011]. DoDI 5200.33 provided under separate cover.

11l(1): All Visit Access Requests (VARs) by Contractors shall be sent via the Joint Personnel Adjudication System (JPAS) to the DISA VAR Center (JPAS SMO:DKABAA10) or appropriate Security Management Office (SMO) for the effort. The COR/TM must be notified and approve the VAR and need to know certification prior to sending the request to the facility being visited. Contractors must also provide a copy of the VAR to the security manager.



11I(2): The Contractor will comply with the Information Assurance (IA) requirements contained in the contract. Minimum IA requirements provided under separate cover.

11I(3): The Contractor will include all DD-254 requirements in all subcontracts necessary to delivery COMSATCOM services meeting the requirements contained in the contract and in this DD-254 (e.g., vendor providing satellite bandwidth for a specific Task Order). Contractor will ensure Subcontractor compliance with all DD-254 requirements.

General Information:

The COR/TM must be notified and approve the receipt and/or generation of classified information under this contract.

All classified information received and/or generated under this contract is the property of the U.S. Government regardless of proprietary claims. Upon completion or termination of this contract, the U.S. Government will be contacted for destruction or disposition instructions.

(END OF ATTACHMENT J-15)