1. ***Security Agreement (SA).*** The contractor shall enter into a security agreement if service performance is on base. This agreement shall outline how the contractor integrates security requirements for service operations with the Air Force to ensure effective and economical operation on the installation. The agreement shall include:

a. Security support provided by the Air Force to the contractor shall include storage containers for classified information/material, use of base destruction facilities, classified reproduction facilities, use of base classified mail services, investigation of security incidents, and the use of security forms and conducting inspections required by DoDM 5220.32 Vol 1, *National Industrial Security Program: Industrial Security Procedures for Government Activities,* Air Force Policy Directive 16-14, *Security Enterprise Governance,* and Air Force Manual 16-1406, *National Industrial Security Program: Industrial Security Procedures for Government Activities.*

b. Security support requiring joint Air Force and contractor coordination includes packaging classified information, mailing and receiving classified materials, implementing emergency procedures for protection of classified information, security checks and internal security controls for protection of classified material and high-value pilferable property.

c. On base, the long-term installation security agreement may take the place of a *Standard Practice Procedure* (SPP).

2. ***Obtaining and Retrieving Identification Media.***

a. DoD Common Access Card (CAC), (AFI 36-3026 Vol 2, *Common Access Card*), used for contracts for more than six months and requirement exists for access to the government computer systems and software. CAC applications are accomplished by Trusted Agents via the Trusted Agent Sponsorship System (TASS).

3. ***Security Clearance Requirements.*** The contractor must possess or obtain an appropriate facility security clearance, (Top Secret, Secret, Confidential) prior to performing work on a classified government contract. If the contractor does not possess a facility clearance the government will request one. The government assumes costs and conducts investigations for Top Secret, Secret, and Confidential facility security clearances. The contractor shall request personnel security clearances, at the company's expense, for employees requiring access to classified information within 15 days after receiving a facility clearance or, if the contractor is already cleared, within 15 days after service award. Due to costs involved with security investigations, requests for personnel security clearances shall be kept to the minimum amount employees required to perform contract requirements.

4. ***List of Employees.*** The contractor shall maintain a current list of employees. The list shall include employee's name, social security number, and level of security clearance. The list shall be validated and signed by the company *Facility Security Officer* (FSO) and provided to the contracting officer and *Information Protection Office* (IP Office) at each performance site 30

days prior to the service start date. Updated listings shall be provided when an employee's status or information changes. A Visit Request for all employees with a security clearance is required to be sent through the Defense Information System for Security (DISS) or successor system, and must be updated at least annually. The contractor shall notify the Information Protection Office at each operating location 30 days before on-base performance of the service. The notification shall include:

a. Name, address, and telephone number of company key management representatives.

b. The contract number and contracting agency.

c. The highest level of classified information to which employees require access.

d. The location(s) of service performance and future performance, if known.

e. The date service performance begins.

f. Any change to information previously provided under this paragraph.

5. *Suitability Investigations.* Contractor personnel not requiring access to classified shall successfully complete, as a minimum, a Tier 1 (T1) investigation, before operating government furnished workstations. The contractor shall comply with the DoDM 5200.02*, Procedures for the Department of Defense Personnel Security Program* and AFI 17-130, *Cybersecurity Program Management,* requirements. T1 investigation requests are initiated using the Standard Form (SF) 85 and are submitted to the installation Information Protection Office through the using agency's Security Assistant (SA). T1 investigations are different from the Wants and Warrants checks, and are provided by the government at no additional cost to the contractor.

For contracts requiring IT-Level I and II access with no access to classified material, the contractor shall complete Tier 5 (T5) formerly called an SSBI or Tier 3 (T3) investigations, respectively. These investigations are submitted using the SF 86, and are submitted to the Information Protection Office through the using agency Unit Security Assistant within five calendar days after contract start. These investigations are provided by the government at no additional cost to the contractor.

6. *Security Monitor Appointment.* The contractor shall appoint a security representative for the on base long term visitor group. The security representative may be a full-time position or an additional duty position. The security representative shall work with the host organization to provide employees with training required by DoDM 5200.01, *Information Security Program,* AFPD 16-14, *Security Enterprise Governance,* and AFI 16-1404, Air *Force Information Security Program*. The contractor shall provide initial and follow-on training to contractor personnel who work in Air Force controlled/restricted areas. Air Force restricted and controlled areas are explained in AFI 31-101, *Integrated Defense.*

7. ***Additional Security Requirements.*** In accordance with DoDM 5200.01, *Information Security Program* and AFMAN 16-1404, the contractor shall comply with local communications squadron policy.

8. ***Freedom of Information Act Program (FOIA).*** The contractor shall comply with DoD Manual 5400.07_AFMAN33-302, *DoD Freedom of Information Act Program,* requirements.

9. ***Reporting Requirements.*** The contractor shall comply with AFI 71-101, Volume- 1, *Criminal Investigations,* and Volume-4, *Counterintelligence,* requirements, as referenced in AFMAN 16-1406, para 2.2.e.

10. ***Physical Security.*** Areas controlled by contractor employees shall comply with AFI 31-101

11. ***Operating Instructions.*** For controlled areas used exclusively by the contractor, the contractor shall develop an Operating Instruction (OI) for internal circulation control, protection of resources and to regulate entry into Air Force controlled areas during normal, simulated and actual emergency operations. The OI shall be written in accordance with AFI 31-101, and coordinated through the Information Protection (IP) office.

12. ***Lock Combinations.*** The contractor shall comply with DoDM 5200.01, Vol 3 security requirements for changing combinations to storage containers used to maintain classified materials.