TAFB Security Requirements

1. Security Requirements. Travis Air Force Base is designated as a closed base. In order to promote security and safety, all contractors desiring access must adhere to installation entry requirements, to include, identity proofing and vetting. This includes a National Crime Information Center (NCIC) and California Law Enforcement Telecommunication System (CLETS) check. Identity proofing and vetting is not required for contractors if they have a current favorable government security clearance which can be verified through the Joint Personnel Adjudication System (JPAS).

2. The primary contractor will ensure all contractors possess proper credentials allowing them to work in the United States and ensure illegal aliens are not employed and/or transported onto the installation. At least one of the following forms of identification will be required for identity proofing:

United States Passport
Permanent Registration Card/Alien Registration Receipt Card (Form I-551)
Foreign Passport with a temporary (I-551) stamp or temporary (I-551) printed notation on a machine readable immigrant visa.
Employment authorization document that contains a photograph (Form I-766)
Current/valid Driver's License (see para. 3)
Identification card issued by Federal, State or local Government
U.S. Coast Guard Merchant Mariner Legacy Card
U.S. Coast Guard New Merchant Mariner Credential

Additional supplemental sources of identity proofing which may be requested during increased Force Protection Conditions (FPCONs) or Random Antiterrorism Measures (RAMs) include, but are not limited to:

School identification card with photograph
U.S. Military or draft record
Native American Tribal Document
U.S. Social Security Card issued by the Social Security Administration (SSA)
Certification of Birth Abroad issued by the Department of State (Form FS-545 or Form DS-1350)
Original or certified copy of a birth certificate issued by a state, county, municipal authority or outlying possession of the United States bearing an official seal
U.S. Citizen ID Card (Form I-197)
ID Card for use of Resident Citizen in the United States (Form I-179)
Unexpired employment authorization document issued by the Department of Homeland Security (DHS) which includes, a) Form I-94 identifying the holder as an asylee, or b) other documentation issued by DHS or the former Immigration and Naturalization Service that

identifies the holder as an asylee, lawful permanent resident, refugee or other status authorized to work in the United States incident to status Foreign Military or Government Identification Credentials Foreign passport with a current arrival-departure record (Form I-94) bearing the same name as the passport and containing an endorsement of the alien's nonimmigrant status, if that status authorizes the alien to work for the employer In the case of a nonimmigrant alien authorized to work for a specific employer incident to status, a foreign passport with Form I-94 or Form I-94A bearing the same name as the passport and containing an endorsement of the alien's nonimmigrant status, as long as the endorsement has not yet expired and the proposed employment is not in conflict with
any restrictions or limitations identified on the form. The contractor shall not be entitled to any compensation for delays or expenses associated with complying with the provision of this clause. Furthermore, nothing in this clause shall excuse the contractor from proceeding with the contract as required.

3. The REAL ID Act of 2005 established minimum standards for the production and issuance of state-issued driver's licenses and ID cards which include requirements for a photograph and certain biographic information, such as name, date of birth, gender, height, eye color, & address. State issued driver's licenses and ID cards from states not meeting the standards can no longer be used for accessing Federal facilities including Air Force installations unless the issuing state's compliance deadline has been extended by the Department of Homeland Security (DHS). State compliance with the REAL ID Act can be found at: https://www.dhs.gov/current-status-states-territories. Contractors with a CA driver licenses and ID cards without any markings in the upper left hand corner are sufficient for identity proofing without supplemental sources until 1 Oct 20. Contractors with a CA driver licenses and ID cards with a gold bear in the upper left corner and are considered sufficient for identity proofing without supplemental sources indefinitely. Contractors with a CA driver licenses and ID cards with "Federal Limits Apply" in the upper left corner is not considered sufficient for identity proofing without supplemental sources. Supplemented sources as specified in para. 2. Contractors from states which are in compliance, or has an approved extension, may use their state-issued driver's license may be used for identity proofing. Contractors from states which are not in compliance, must use an alternative identification credential for identity proofing as specified in para. 2. Contractors from states which are not in compliance and do not have an alternative identification credential must be escorted or denied access.

4. Identity Proofing and Vetting. Contractors will be identity proofed and vetted each time a pass is issued. Security Forces may conduct random screenings at any time. If disqualifying base access information is found contractors may be denied base access or have passes currently issued revoked.

Following are the base access disqualifiers:

The individual is known to be or reasonably suspected of being a terrorist or belongs to an organization with known terrorism links/support.
The installation is unable to verify the individual's claimed identity.
The individual has previously been barred from access to a federal installation or stand-alone facility.
The individual is wanted to Federal, State, or other civil law enforcement authorities, regardless of offense or violation.
The individual has any conviction for espionage, sabotage, treason, terrorism, or murder.
The individual's name appears on any Federal or State agency's watch list, hit list or registration list for criminal behavior or terrorist activity.
The individual has been convicted of a firearms or explosive violation.
The individual has been convicted of sexual assault, armed robbery, rape, child molestation, child pornography or trafficking in humans.
The individual has been convicted of drug possession with intent to sell or drug distribution.
The individual has knowingly and willfully engaged in acts or activities designed to overthrow the U.S. Government by force.
Within the past 10 years, the individual has been convicted of 2 or more felonies, or 2 or more violent misdemeanors, or 1 or more felonies and 1 or more violent misdemeanors.
There is reasonable basis to believe on an individual's extensive and systemic criminal behavior, that issuance of an access credential poses an unacceptable risk to the installation. Extensive criminal behavior is a large amount of police arrests and/or convictions from age 18 to present. Systemic criminal history is a consistent interval of police arrests and/or convictions from age 18 to present. Contractors with disqualifying base access information will be issued a denial access letter immediately revoking their base access privileges.
Contractors requesting a denial modification must submit a written rebuttal/request within 10 business days of receipt of the denial of access letter to 60 SFS/CC, Attention: 60 SFS/S5R, Bldg 381, 540 Airlift Drive, Suite C-101, Travis AFB 94535-2451.

5. Primary Contractor Responsibilities. The primary contractor will be responsible for the conduct of all contractors employed or sponsored. Additionally, the primary contractor will: Coordinate base entry requirements with the 60th Contracting Squadron. Advise contractors working on the installation they are subject to identity proofing and vetting against an authorized data base for criminal history as specified herein. Advise contractors base passes are only valid for the purpose, person and vehicle for which it was issued. Use of the base pass for any other purpose or by any other person will result in personnel being denied access and the pass confiscated. Additionally, contractors which misuse their pass may be subject to debarment actions. If a pass is lost, notify the Pass and Registration Office immediately. Provide written notification, within 24 hrs, to the 60th Contracting Squadron of any changes in employee's status. This includes, but is not limited to, the employee being fired or quitting their position with the company. Retrieve passes from contractors which no longer need installation access. Passes will

be turned into the 60th Contracting Squadron upon expiration. If a contractor was terminated for cause, notify the Pass and Registration Office immediately.

6. Obtaining a Base Pass. Provide an EAL (Entry Authority List) of all contractors on company letterhead which require a base pass. All requests for a base pass will be submitted through the Base Contracting Office NLT 45 days prior to the contract start date. Exceptions will be made for short-notice contracts where the award date and performance start date are less than 45 days. A base pass will be issued for the length of the contract, not to exceed one year. Prior to renewing a base pass, return the old base pass to the Pass and Registration Office for destruction. Ensure the EAL includes: Contract number Work site or location Inclusive dates of the contract Work schedule (include days of the week and time periods contractors are on base) Employee's full name, date of birth, and social security number

7. Contractor Responsibilities. All contractors requiring reoccurring and unescorted access onto the installation must: Have within their possession the identification used to obtain a pass and the pass issued. Register privately owned vehicles in accordance with installation policies. On request, present identification or installation pass to base police. Refusal may result in denial of installation access. Turn in passes to the 60th Contracting Squadron when expired or no longer required. If a contractor was terminated for cause, notify the Pass and Registration Office immediately.

8. Increased Force Protection Condition (FPCON). During FPCON Normal, Alpha and Bravo; contractors without a base issued pass must be sponsored onto the installation. During FPCON Charlie and Delta the base will curtail non-essential operations/functions and non-essential contractors will be suspended at the direction of the installation commander. All contractors attempting installation access; thereafter, will be physically escorted unless FPCON Mission-Essential designation has been approved in advance and is indicated on the base pass.

9. Restricted Area Badges (RAB). Contractors may be submitted for unescorted entry into restricted areas if required for their contract. The security manager of the agency responsible for the project will assist, as appropriate.

10. Escort Requirements. The following escort requirements apply: While on the installation, sub-contractors must be escorted at all times. While within Restricted or Controlled Areas contractors not in possession of a restricted area badge will be escorted at all times. Escorts can be either the military agency responsible for the project or contractor in possession of a restricted area badge.

11. Lost Base Passes or Restricted Area Badges. The Primary Contractor will investigate and provide written notification to the 60th Contracting Squadron anytime a base pass is lost. Notification should include an explanation from the employee on how, when, where and what

steps have been taken to locate the missing pass. If a replacement is needed, forward the notification with the request for a base pass. The Primary Contractor must immediately report the loss of RAB to the security manager of the military agency that submitted the RAB request. The individual who lost the RAB will provide a written explanation on how, when, where and what steps have been taken to locate the missing RAB. The security manager will conduct their own inquiry and forward a report of investigation [with squadron commander endorsement]; the member's written explanation and the original AF Fm 2586 to the Pass and Registration office. A new RAB will not be issued until the investigation is complete.

12. Information Protection Security Training. IAW DoDM 5200.01, Volume 3, Enclosure 5 and AFI 16-1404, para 2.8.3, Security Managers ensure initial orientation and refresher training is conducted for all personnel. This includes specialized security training. The security manager is required to track and document the completed training. The contractor will be required to participate in the government's in-house and web-based security training program under the terms of the contract. The government will provide the contractor with access to the on-line system after appropriate vetting qualifications have been met.

13. Controlled Unclassified Information. Agency information marked "For Official Use Only" or bearing other sensitivity marking will be handled in accordance with agency information security program regulations and instructions. This information will not be divulged or disclosed without agency permission. Contractor personnel will ensure information that is considered sensitive or proprietary is not compromised.

14. Visitor Group Security Agreement (VGSA). IAW AFI 16-1406, Chapter 4. At the request of the Installation Commander (IC) the contracting officer reserves the right to execute a VGSA agreement with all contractor operations located on Travis AFB that require access to classified information. Furthermore, at the discretion of the IC the VGSA execution requirement may be extended to contractors performing on contracts that require access to sensitive unclassified information, sensitive resources or frequent "entry" to the installation.

15. Antiterrorism Force Protection Training. IAW AFI 10-245 and Force Protection Plan 31-1, all employees with contracts over 90 days, will complete initial Level I Antiterrorism Awareness training at https://jkodirect.jten.mil/Atlas2/page/login/Login.jsf. To ensure security measures, at a minimum, shall address elements such as contractor screening, access control, favorable fingerprint or National Crime Information Center (NCIC) results, circulation control special security concerns, and training. Thereafter, Level I Antiterrorism Awareness training will be completed annually. All personnel will be responsible to provide proof (copy of training certificates) of training to the Antiterrorism Representative (ATRs) responsible for the unit they are contracted.

16. Operations Security (OPSEC). IAW AFI 10-701, 60 AMW will consider OPSEC for all contractual requirements and determine if any contract contains any form of critical and/or sensitive information or activities. These requirements will be defined on the contract and

SOW/PWS. If OPSEC requirements exist, the organization's OPSEC Coordinator or the 60 AMW OPSEC Program Manager will be contacted to review the SOW/PWS. This review may result in possible training requirements, in addition to what is stated below. For unclassified contracts, the DD Form 254, Department of Defense Contract Security Classification Specification, can be used to specify OPSEC requirements in lieu of defining these requirements on the contract and SOW/PWS. For classified contracts, the DD Form 254 is mandatory. Additionally, the 60 AMW OPSEC Program Manager or functional Unit OPSEC Coordinator will provide OPSEC training or training materials to contract employees within 90 days of employees' initial assignment to the contract. (AFI 10-701, 5.2.4). The Installation (60 AMW) OPSEC Program Manager can be contacted at 424-4355 or 3261.

DISQUALIFYING CRITERIA FOR INSTALLATION ACCESS

A. The individual is known to be or reasonably suspected of being a terrorist or belongs to an organization with known terrorism links/support.

B. The installation is unable to verify the individual's claimed identity.

C. The individual has previously been barred from access to a federal installation or stand-alone facility.

D. The individual is wanted by Federal, State or other civil law enforcement authorities, regardless of offense or violation.

E. The individual has any conviction for espionage, sabotage, treason, terrorism, or murder.

F. The individual's name appears on any Federal or State agency's watch list or hit list for criminal behavior or terrorist activity.

G. The individual has been convicted of a firearms or explosive violation.

H. The individual has been convicted of sexual assault, armed robbery, rape, child molestation, child pornography, trafficking in humans, drug possession with intent to sell, or drug distribution.

I. The individual has knowingly and willfully engaged in acts or activities designed to overthrow the U.S. Government by force.

J. Within the past 10 years, the individual has been convicted of 2 or more felonies, or, 2 or more violent misdemeanors, or 1 or more felonies and 1 or more violent misdemeanors.

K. There is reasonable basis to believe based on an individual's extensive and systemic criminal behavior, that issuance of an access credential poses an unacceptable risk to the installation/mission. Extensive criminal behavior is a large amount of police arrests and/or convictions from age 18 to present. Systemic criminal history is a consistent interval of police arrests and/or convictions from age 18 to present.