ATTACHMENT A – GENERAL INSTALLATION SECURITY REQUIREMENTS

1. **SECURITY REQUIREMENTS**

All Military Installations are designated as a closed base. In order to promote security and safety, all employees 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 employees if they have a current favorable government security clearance which can be verified through the Joint Personnel Adjudication System (JPAS).

The prime contractor will ensure all employees 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-1551)
- Foreign Passport with a temporary (I-1551) stamp or temporary (I-1551) printed notation on a machine readable immigrant visa.
- Employment authorization document that contains a photograph (Form I-766)
- Current/valid Driver's License
- 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 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 requirement. Furthermore, nothing in this requirement shall excuse the contractor from proceeding with the contract as required.

2. **IDENTITY PROOFING AND VETTING**

Employees whose background reveals any of the following disqualifiers will not be allowed installation access. All employees will be vetted based on the following disqualifying base access criteria:

- The installation is unable to verify the individual's:
  - Citizenship, immigration status, or social security number or claimed identity.

- The individual is/has/has been:
  - Barred from entry/access to a federal installation or facility.
  - Wanted by federal/civil law enforcement authorities, regardless of offense/violation.
  - On a federal agency "watch list" or "hit list" for criminal behavior/terrorist activity.
  - Knowingly/willfully engaged in acts/activities to overthrow the government by force.
  - Incarcerated 12 months/longer in the past 10 years, regardless of offense/violation, unless released on proof of innocence.

- The individual has been convicted of:
  - Child molestation or pornography; any crime involving indecent acts with a minor.
  - Espionage, sabotage, treason, terrorism, or murder.
  - Firearms or explosive violation within the past ten years.
  - Felony involving violence against a person, arson robbery or burglary.
  - Drug distribution, possession, intent to sell, trafficking or use more than once.
  - Sexual assault, rape, human trafficking or any felony sexual in nature requiring registration as a sex offender under applicable federal or state law.

- The individual is known to be or reasonably suspected of:
  - Being a terrorist or belongs to an organization with known terrorism links or support.

- There is reasonable basis to believe the individual:
  - Submitted fraudulent information concerning his or her identity.
  - Will unlawfully or inappropriately use an access credential outside the workplace.
  - Will attempt to gain unauthorized access to classified documents, information protected by the Privacy Act, information that is proprietary in nature, or other sensitive or protected information.

- There is reasonable basis to believe, that issuance of an access credential poses unacceptable risk when:
  - Criminal or dishonest history exists.
  - A statutory or regulatory bar prevents the individual's contract employment; or would prevent federal employment.
  - The individual's material, intentional false statement, deception or fraud in connection with federal or contract employment.
  - Based on the nature or duration of the individual's alcohol abuse without evidence of substantial rehabilitation.
  - Based on the nature or duration of the individual's illegal use of narcotics, drugs, or other controlled substances without evidence of substantial rehabilitation.

Employees 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 employees may have their passes revoked.

Employees with disqualifying base access information will be issued a denial access letter immediately revoking their base access privileges. Employees requesting to contest the adjudication, denial of installation access, or requesting a

waiver/exception to policy must submit a written rebuttal/request within ten (10) business days of receipt of the barment letter to the specific Air Force, Joint Base, or ANG Installation office designated on the letter.

3. **PRIMARY CONTRACTOR RESPONSIBILITIES**

The prime contractor will be responsible for the conduct of all employees working under that contract. Additionally, the primary contractor will:

Coordinate base entry requirements with the specific Military Installation office. The COR and USACE PM shall be copy furnished on all installation communications.

Advise employees working on the installation they are subject to identity proofing and vetting against criteria specified in item 2. Any employee who does not complete or sign the form will be denied installation access.

Advise employees 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 the pass being confiscated. Employees who misuse their pass may be subject to barment actions. If a pass is lost, notify the Pass and Registration Office immediately.

- To obtain a pass, personnel will need a valid state or government photo identification.

- To obtain a vehicle pass, personnel will need a driver license, registration and insurance.

Provide written notification, within 24 hrs, to the Installation's Security Office 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 government issued personal and vehicle passes from employees which no longer need installation access. Passes will be turned into the Installation Security office upon expiration.

4. **OBTAINING A BASE PASS**

Provide an EAL (Entry Authority List) of all employees on company letterhead, which require a base pass. All requests for a base pass will be submitted through the Installation's Security Office or the Installation POC. A base pass will be issued for a maximum of one (1) year. Prior to renewing a base pass, return the old base pass to the Pass and Registration 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 employees are on base)
- Employee's full name, date of birth, and social security number

Only persons who have undergone identity proofing and vetting and have no disqualifying base access information can serve as a sponsor. Persons appointed as sponsors will meet employees at the Visitor Control Center and ensure they are advised of security language contained herein.

5. **EMPLOYEE RESPONSIBILITIES**

All employees requiring reoccurring and unescorted access onto the installation must:

- Carry their DoD ID card or installation pass on their person while on the installation.
- Register privately owned vehicles in accordance with installation policies.
- On request, present their DoD ID card or installation pass to security personnel. Refusal may be grounds for further administrative or punitive action.
- If issued a Command Access Card (CAC), present documentation from the local security office or CAC sponsor confirming that the CAC has been reported lost or stolen.
- Turn in access credentials to the Installation when the credential expires or when the basis for obtaining the credential no longer exists.

6. **INCREASED FORCE PROTECTION CONDITION (FPCON)**

During FPCON Normal, Alpha and Bravo; employees 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 employees will be suspended at the direction of the installation commander. All employees 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.

7. **CONTROLLED/RESTRICTED AREAS**

Employees not in possession of a restricted area badge will be escorted at all times when working within controlled, restricted or other sensitive areas. Escorts can be either installation personnel responsible for the project or an employee in possession of a restricted area badge. The Installation personnel or employee in possession of a restricted area badge will follow existing procedures and instructions for obtaining entrance to controlled, restricted and sensitive areas. Employees may be submitted for unescorted entry into restricted areas, if required for their contract.

8. **LOST BASE PASSES OR RESTRICTED AREA BADGES**

Base Passes - The employee's supervisor will investigate and provide written notification for a lost base pass to the Installation Security Office. Written notification should include an explanation from the employee on how, when, where and what steps have been taken to locate the missing base pass. If a replacement is needed, forward the notification with the request for a base pass.

Restricted Area Badges (RAB) - Employees issued a RAB must report the loss immediately 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; the member's written explanation and the original AF Form 2586 to the Pass and Registration office. A new RAB will not be issued until the investigation is complete.
For Official Use Only 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.