EXHIBIT F
AEDC SITE OPERATIONAL CONDITIONS

Arnold Engineering Development Complex (AEDC) at Arnold Air Force Base (AAFB) operates within a unique environment. Some site operational conditions may be the same or similar to other Air Force installations; however, some are very different due to the AEDC Mission, base populace composition, and multiple other weighted factors. The Test Operations & Sustainment (TOS) Contractor is the prime contractor and constitutes most of the AEDC workforce. TOS must ensure on behalf of the Air Force that all TOS Subcontractors are informed and adhere to AEDC operational conditions, as prescribed herein.

AAFB MISSION AREA ENTRY & CIRCULATION CONTROL

In order to support a determination regarding whether an individual requesting base entry presents a threat to good order, discipline and morale at AAFB, the Security Services Contractor (SSC) is authorized to perform a triple I on any individual requesting entry onto AAFB using the Tennessee Information Enforcement System (TIES), National Crime Information Center (NCIC), OpenFox, and the State of Tennessee Integrated Criminal Justice Portal (CJP).

All violations of AAFB rules and regulations are reported by the SSC to the Air Force and the responsible contracting organization for appropriate disciplinary action or referred to the appropriate civil authorities for action/disposition.

Each Subcontractor employee is required to have proper circulation control passes or badges to enter the AAFB fenced Mission Area (MA). The AAFB Visitor Control Center (VCC), located adjacent to the Main Gate, in Building 111 is responsible for issuing these credentials. The VCC is operated by the CSS. Contractor will support Subcontractor's request for site access but has no control over the VCC operations and will not be responsible for any delays or increased costs incurred by Subcontractor that result from the VCC operations.

The TOS Subcontract Administrator will provide the VCC a completed AEDC Form 898, Contractor Clearance Request, to identify subcontractor employees. AEDC Form 898 must identify person(s) authorized to complete the AEDC 900, Contractor Employment Notice. AEDC Form 900 is used to request the unescorted entrance of subcontractor employees to perform work at AEDC. The subcontractor representative, also known as the site superintendent, will provide an updated AEDC Form 898 listing each employee that requires access prior to the start of a subcontract. The VCC will not issue badges without this documentation or a current AEDC Form 898 on file.
Once issued, credentials must be presented at the gate for entry. Subcontractor badges have a white background with photo, name, AEDC Crest, barcode, expiration date, employee identification (ID). Badges must be displayed on the front of an outer garment, above the waist with the photograph visible at all times within the fenced area. The badge may be worn on a necklace/chain provided the badge remains visible outside the outer garment, above the waist, and the picture is shown outward. AEDC personnel will challenge Subcontractor personnel, who are not displaying proper credentials; if credentials cannot be produced, the CSS will be notified immediately.

If displaying the badge on the outer garment in the immediate work area will create a safety hazard, then the badge can be removed and placed in the pocket of the individual. Upon departure of the immediate area, the badge will be displayed.

AEDC credentials are the property of the U.S. Government. Subcontractors must promptly return credentials to the VCC upon termination of the services of each of its employees. Subcontractors must immediately report to the Contractor any loss of employees' credentials.

Upon subcontract completion (to include employment termination), and before final payment can be made, the subcontractor shall ensure all badges have been turned into the issuer at VCC. Subcontractor employees terminating employment for any reason shall return all ID badges prior to departing the base. If the subcontract has been extended, contact the VCC to ensure the expiration date is extended.

VISITORS AND LOWER TIER SUBCONTRACTORS

To expedite entry into the MA, during normal duty hours, call the VCC at (931) 454-5453. During non-duty hours, call the Base Defense Operations Center (BDOC) at (931) 454-5662. Only the authorized subcontractor representative can authorize visitors (U.S. citizens) in conjunction with the specific subcontract.

Subcontractors that sponsor a lower tier subcontractor's visit shall receive an endorsement from the Contractor or Department of Defense (DoD) representative and comply with specified requirements.

The subcontractor shall comply with all security regulations and directives as identified herein and other security requirements shown elsewhere in this subcontract. These requirements apply to all subcontractors working on AAFB that DO NOT have access to classified information in the performance of their subcontract. AEDC is a closed military installation; therefore, the below requirements and procedures are prerequisites to the issuance of any subcontractor identification. Subcontractor requests for exceptions to the below requirements and procedures shall be addressed to the Subcontract Administrator who will obtain an approval or disapproval from the Complex commander who has the final authority on access issues. The AEDC Complex reserves the right to refuse entry and/or re-entry of any person to AEDC for just cause to protect personnel, facilities, and property under his control through the use of a debarment order when such actions are deemed necessary.

a. As stated above, all visitors at AEDC will be screened through multiple checks to determine if there are outstanding warrants or criminal involvement. Anyone with an active warrant will be denied entry and, if extradition is approved, taken to jail. Persons identified as having a violent criminal past or gang affiliation will be denied entry regardless of warrant status.

b. Examples that may disqualify someone from entering the installation include, but are not limited to, the following:

1. Identity, U.S. citizenship, immigration status, or Social Security Account Number cannot be verified.
2. There is a reasonable basis to believe the individual has submitted fraudulent information concerning his or her identity.
3. Previous debarment from entering/accessing any other military base or facility.
4. There is a reasonable basis to believe that the individual 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.
5. Failure to safeguard Controlled Unclassified Information.
6. There is a reasonable basis to believe that the individual will or inappropriately use an access credential outside the workplace.
7. There is a reasonable basis to believe, based upon an individual's criminal or dishonest history, that issuance of an access credential poses an unacceptable risk to the installation/mission.
8. There is a reasonable basis to believe, based upon the individual's material, intentional false statement, deception, or fraud in connection with Federal or contract employment, that issuance of an access credential poses an unacceptable risk to the installation/mission.
9. The individual is wanted by Federal or civil law enforcement authorities, regardless of offense or violation.

10. Conviction of firearms or explosives violation or any conviction of espionage, sabotage, treason, terrorism, or murder
11. Conviction of violent crimes, e.g., sexual assault, armed assault/robbery, rape, child molestation or kidnapping, or human trafficking, etc.
12. Drug possession with intent to sell or distribute.
13. Name appears on any federal agency's "watch list" or "hit list" for criminal behavior or terrorist activity.
14. Known to be or reasonably suspected of having affiliation in any gang, hate group, or terrorist organization.
15. Advocating or affiliating with any organization or group that advocates or defends the overthrow of the U.S. Government by force.
16. Willfully hindering or limiting base and service operations such as investigations, fire, police response, and operations.
17. Introducing, transporting, using, or simply possessing ammunition, firearms, explosives, or other lethal weapons in the AEDC fenced MA, except where and when authorized.
18. Using privately owned radio-transmitting equipment within areas where use is prohibited and posted.
19. Stealing (or possessing without proper authority) Government or Contractor property, or property of another.
20. Gambling, dishonesty, and other actions deemed illegal by law.
21. Disregarding safety rules and common safety practices.
22. Failing to observe traffic, parking rules and requirements.
23. Failing to immediately report a Contractor or private motor vehicle accident to Installation Security Personnel.
24. Use of tobacco products where or when prohibited and/or using "strike anywhere" matches.
25. Willfully disregarding fire protection rules or requirements, to include tampering with fire extinguishers, fire protection systems, or other fire protection equipment.
26. There is a reasonable basis to believe, based on the nature or duration of the individual's alcohol abuse without evidence of substantial rehabilitation, that issuance of an access credential poses an unacceptable risk to the installation/mission.
27. There is a reasonable basis to believe, based upon the nature or duration of the individual's illegal use of narcotics, drugs, or other controlled substances without evidence of substantial rehabilitation, that issuance of an access credential poses an unacceptable risk to the installation/mission.
28. A statutory or regulatory bar prevents the individual's contract employment, or would prevent Federal employment under circumstances that furnish a reasonable basis to believe that issuance of an access credential poses an unacceptable risk to the installation/mission.

Additionally, the Commander reserves the right to deny access to any visitor, with proper justification. This authority enables the commander to fulfill responsibilities to protect personnel and property, to maintain good order and discipline, and to ensure the successful, uninterrupted performance of the Air Force mission.

SECURITY REPORTING

Subcontractor personnel shall report to an appropriate authority, any information or circumstances of which they are aware that may pose a threat to the security of DoD personnel, contractor personnel, resources, and classified or unclassified defense information. Reports may be made to the BDOC at 931-454-5662, the Mission Support Division/security forces (AEDC/TSD-SF), at 931-454-3424/7610 or the Air Force Office of Special Investigations at 931-454-7820.

CAMERA, PHOTOGRAPHY, WEB CAMERA AND ELECTRONIC EQUIPMENT GUIDELINES

Use of private cameras, to include cell phones, inside the MA is not allowed in areas marked as "No Photography." If photographs of the job site are needed, subcontractors must contact the job monitor or the Subcontract Administrator; subcontractors must not use cell phones to capture images for operational

security (OPSEC) purposes. Professional quality photo support can be provided by the base photo lab. Use of cameras in administrative areas is generally permitted as long as sensitive information and badges are not captured in images.

a. Photography equipment is defined as any device capable of capturing or recording an image or likeness and is prohibited in posted areas of AEDC, including AEDC White Oak Facility and NFAC. The use/possession of portable electronic devices with cameras, recording (to include voice) are prohibited without written authorization from the Air Force within posted facilities. This policy does not apply to use of video surveillance systems approved under other DoD directives.

CELL PHONE USAGE

Vehicle operators on an AF installation and operators of privately owned, government owned, leased, or rented vehicles, on or off an AF installation, shall not use cell phones while the vehicle is in operation, except when using a hands-free device or hands-free operating mode. When possible, vehicle operators should pull over and place the vehicle in park before using any cell phone. Land Mobile Radios (LMR) are primarily listening devices and are not restricted. Cell phones and other devices, used only in push-to-talk (walkie-talkie, direct connection) mode are considered LMR if issued for the performance of official duties.

a. Wearing portable headphones, earphones, or other listening devices while operating a motor vehicle, running, jogging, walking, bicycling, or skating (e.g. roller skates, roller blades, skateboards, etc.) on AF installation roadways is prohibited, with the exception of a hands-free telephone headset or single-bud earpiece. This does not include the use of hearing aids, nor does it negate the requirement for wearing hearing protective equipment where conditions dictate their use. EXCEPTION: Motorcycle helmet intercom system between operator and passenger is permitted.

b. This does not negate the requirement for wearing hearing protection when conditions or good judgment dictate use of such protection such as the wear of hearing protection as required in high noise areas.

c. Vehicle operators will not engage in text messaging while driving a vehicle.

d. Violating this policy is considered a “primary offense.” This means violators will be stopped solely for this offense. Cell phones (private or subcontractor owned) are authorized for use on AAFB except within posted facilities and/or areas where Facility Managers, Security or Safety has posted a policy prohibiting their use.

INFORMATION PROTECTION

a. This clause applies to the extent that this Subcontract involves access to information classified “Confidential,” “Secret,” or “Top Secret.”

b. The Subcontractor shall comply with (1) their DD Form 441, DoD Security Agreement, including DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), and (2) any revisions to that manual, notice of which has been furnished to the Subcontractor.

c. If, subsequent to the date of this Subcontract, the security classification or security requirements under this Subcontract are changed by the Government and if the changes cause an increase or decrease in security costs or otherwise affect any other term or condition of this Subcontract, the Subcontractor shall be subject to an equitable adjustment, as if the changes were directed under the Changes clause of the Subcontract.

d. The Subcontractor agrees to insert terms that conform substantially to the language of this clause, including this paragraph 4 but excluding any reference to the Changes clause of this Subcontract, in all lower-tier Subcontracts under this Subcontract that involve access to classified information, and shall, in a timely manner, notify the Contractor Security Office as indicated in Block 16 of the DD Form 254, DoD Contract Security Classification Specification, of any lower-tier Subcontracts under this Subcontract.

Notification of Government Security Activity: Thirty (30) days before the date that Subcontractor operations begin on base, the Subcontractor shall notify the Contractor Security Office as indicated in Block 16 of the DD Form 254, as to:

a. The name, address, and telephone number of the Subcontract's company's representative and designated alternate in the U.S. or oversea area, as appropriate;

b. The Subcontract number and military contracting command;

c. The highest classification category of defense information to which Subcontractor employees will have access;

d. The Air Force installations in the U.S. (in oversea areas identify only the APO number(s) where the subcontract work will be performed

e. The date Subcontractor operations begin on base in the U.S. or in the oversea area;

f. The estimated completion date of operations on base in the U.S. or in the oversea area; and

g. Any changes to information previously provided under this clause

Security Agreement: All Subcontractors performing at AEDC on a classified Contract for more than 90 days must enter into a security agreement either with AEDC TSD/IP or the Contractor Security Office and ensure that their employees are properly trained.

CONTROLLED UNCLASSIFIED INFORMATION

All Controlled Unclassified Information (CUI) developed, used, handled, discussed, or accessed during this Subcontract must be protected adequately, per DoDI 5200.48, Controlled Unclassified Information. Examples of CUI are: Defense; Privacy; Proprietary Business Information; Export Control; Financial; and Critical Infrastructure. Refer to the CUI Registry for the full listing.

Certification by the DLIS JCP is required for all U.S. or Canadian subcontractors who wish to obtain access to unclassified technical data disclosing militarily critical technology with military or space application that is under the control of, or in the possession of the DoD. Certification under the JCP establishes the eligibility of a U.S. subcontractor to receive technical data governed, in the U.S., by DoD Directive 5230.25. To request DLIS Certification subcontractors must submit a DD Form 2345, Military Critical Technical Data Agreement, to the DLIS, Battle Creek, MI address indicated at the top of the DD Form 2345 along with a copy of the company's State Business License, Incorporation Certificate, Sales Tax Identification Form or other documentation, which verifies the legitimacy of the company.

Proprietary Information: In addition to any obligations set forth,

1. Subcontractor hereby agrees that all technical information marked as proprietary contained in documents, drawings, publications, specifications, schedules and the like received from the Contractor for the performance of this Subcontract is received in confidence and is the proprietary

property of the Contractor, and that such information will not be transmitted, reproduced, used, or disclosed to any person or organization by the Subcontractor (except as may be necessary for the performance of work required to be done under this Subcontract with the Contractor) without the express prior written approval of the Contractor.

2. Subcontractor and its employees shall preserve as confidential all information pertaining to the Contractor's or Government's business and all technical and proprietary information obtained from the Contractor or Government in the performance of this subcontract. In the event that a Nondisclosure Agreement has been attached to this subcontract and a conflict arises between this article and the terms of the Nondisclosure Agreement, the terms of the Nondisclosure Agreement shall prevail.

3. No release of any information, or confirmation or denial of the same, with respect to this subcontract or subject matter thereof, will be made without the prior written approval of the Subcontract Administrator. This includes, but is not limited to, advertisements, brochures, and press statements. Any information requested by the Subcontractor for approval of release to the public shall be submitted through the Subcontract Administrator to be processed through the AEDC Public Affairs Process/Office.

Proper Protection of CUI includes:

1. Destruction: When no longer required, CUI must be destroyed by any means that will prevent reconstruction of the material, preferably by cross-cut shredding (if shredded, use equipment that produces no more than ½-inch residue and crosscuts the text so a legible line of text is not produced), or degaussing, or shredding magnetic media. There are locked Shred-It™ Bins across the area in which CUI may be placed for proper destruction. Place only non-CUI/public domain materials such as textbooks, vendor catalogs and instruction booklets, magazines, newspapers, blank papers and forms, specification books and catalogs, telephone books, etc. in Recycle bins.
2. Reproduction: Reproduce CUI on standard office equipment, but ensure all waste, overruns, originals, etc. are properly retrieved and stored or destroyed.
3. Storage/Protection and Access: When unattended, ensure locked protection (desk, office, file cabinet, etc.) of CUI from unauthorized access. If locked protection is unavailable, at a minimum, store CUI out of sight
4. Release of Information:
    a. Need-to-Know must be verified prior to granting access to the information. This includes phone inquiries and unsolicited emails.
        1) Need-to-Know is a determination made by the individual/organization releasing the information that the recipient has a requirement for access to perform tasks or services essential to the fulfillment of the subcontract.
    b. Do not release CUI over open, unsecured communication devices, such as telephones (includes cellular telephones), two-way radios, Blackberry devices, etc.
    c. Do not telefax CUI over an unsecure (unencrypted) telefax machine.
    d. If secure means is unavailable when sending CUI over telefax, then verify the receiving telefax number, have the receiving person standing by at the receiving machine to immediately retrieve the fax, and the sender immediately retrieves the originals from the machine.
    e. When secure communication devices are not readily available or feasible, take precautions by limiting the disclosure of detailed information in a single communication to the greatest extent possible.
    f. CUI must be encrypted prior to transmission over computer lines (email, Internet, etc.).
    g. Do not place CUI or material on an external web site or web page that is accessible to unauthorized personnel (CUI is not approved for release to the public).
    h. Information to be released outside or to the public must complete the Air Force Security Policy and Review process prior to release.

i. Limit Café 100, VCC and other "public use area" discussions to that which is public domain or unofficial business.
j. Foreign Nationals must not have access to CUI that is export controlled. All export control laws must be followed.

OPERATION SECURITY (OPSEC) REQUIREMENTS

The subcontractor will comply with the AEDC OPSEC Program and will protect critical and/or sensitive information per AFI 10-701, Operations Security (OPSEC), and the OPSEC protection guidance provided below. Subcontractor organizations requiring access to unclassified technical data disclosing militarily critical technology with military or space application must be certified with the DLIS JCP prior to access. OPSEC critical information can be released to subcontractor personnel with a valid need-to-know. Contact the AEDC Assistant OPSEC Program Manager at 931-454-4250 or the AEDC OPSEC Program Manager at 931-454-7610 for clarification.

OPSEC Considerations include:

1. Don’t assume Need-To-Know exists between different operating segments within the test customer organization.
2. Don’t acknowledge test customers by their company of employment, or work supported at AEDC, etc. when outside of work environment
3. Whether at AEDC or not, do not acknowledge, confirm or deny the accuracy or legitimacy of U.S. military or other test customer information, whether classified or unclassified.
4. Information being posted on the Internet does not mean it was approved for public release as unclassified and not sensitive.
5. Test schedules, objectives, and results, as directed by the sponsor.
6. Information technologies or systems that, if compromised, would degrade effectiveness, shorten the expected effective life of the system, or significantly alter program direction.
7. Weaknesses in security.
8. Authentication and verification codes, alarm and cipher lock codes and computer passwords as applies to unclassified access.
9. Vulnerabilities or limitations that reflect a capability to meet a real world contingency.
10. Existing or emerging capability, weakness or vulnerabilities.

OPERATIONS AND STORAGE AREAS

Operations of the Subcontractor (including storage of materials while working on a current project) upon Government premises shall be confined to areas authorized or approved by the Contractor. Areas adjacent to the work will be made available for use, by the Subcontractor, without cost whenever such use will not interfere with other Contractor and Government uses or purposes

PHYSICAL SECURITY

Areas controlled by subcontractor employees shall comply with base Operations Plans/Instructions for Force Protection Conditions (FPCON) procedures, Random Antiterrorism Measures and local search/identification requirements.

The subcontractor shall safeguard all property, including controlled forms provided for subcontractor use. At the close of each work period contractor training equipment, ground aerospace vehicles, facilities, support equipment, and other valuable materials shall be secured.

Permission from the building manager **is required prior to roof access of any building at AEDC.**

REMOVAL AND/OR EXCHANGE OF GOVERNMENT PROPERTY

In the event that performance of this Subcontract requires the removal and exchange of Government property at AEDC, the Subcontractor shall coordinate all such activities involving Government property through the Technical Representative/Job Monitor. Each removal of Government property will be accompanied by the appropriate property removal documentation.

In the event Government property is exchanged or replaced by the Subcontractor, such action must be coordinated through the Technical Representative/Job Monitor and approved by the Contractor's Property Office to establish and maintain adequate property control records.

Failure by the Subcontractor to report removal and/or exchange of Government property from AEDC may result in the Subcontractor being liable for the loss and replacement of such property.

CITIZENSHIP / EMPLOYMENT OF FOREIGN NATIONALS

All employees performing on their subcontract must be a **U.S. citizen** or **Registered Alien** and show proof of citizenship. The AEDC host shall require that all Registered Aliens have in their possession their Permanent Resident Cards. A minimum lead-time of 14 business days is required to facilitate timely Permanent Resident Card validation. The visiting Lawful Permanent Resident (LPR) must provide color copies (front & back) of their Permanent Resident Card and their internal passport information (photo/documentation). Visiting LPRs having business with the current base operating Contractor must submit this documentation to the host and Contractor Security Office.

The Contractor Security Office coordinates directly with the AEDC Foreign Disclosure Office (FDO) to complete the validation process and render a recommendation to authorize or deny access. All other visiting LPRs must submit their documentation directly to the FDO via mail (Address: Foreign Disclosure Office, MS-1214, 100 Kindel Drive, Suite A214, Arnold AFB, TN 37389-1214). The FDO provides a list of authorized LPR personnel to the VCC, allowing entry into the applicable areas. Registered Aliens not on an approved list are not be permitted entry into any part of AAFB. If Registered Aliens fail to produce the proper Immigration and Naturalization Service credentials, they are denied access to all portions of AAFB. The subcontractor will be held responsible for complying with federal statutes, which prohibit the hiring of illegal aliens and FNs who are not authorized to work in the United States. Non-U.S. citizens must be identified and present their resident alien cards to VCC to show proof that they have been legally admitted into the United States. Failure to show proof will result in entry being denied.

Employees and/or representatives of companies (U.S. Citizen or FN) under Foreign Ownership, Control, or Influence (FOCI) will be treated and processed as FNs for access to the AEDC MA.

FNs or immigrant/resident aliens shall not be used in performance of this Subcontract without written approval of the Government's Contracting Officer and the AEDC Foreign Disclosure Office (AEDC/XP2). FNs will NOT be approved to perform work requiring access to AEDC computers (networked or stand-alone). Requests to use FNs or immigrant/resident aliens shall be submitted to the Buyer and approval obtained before work commences.

FN subcontractor representatives and employees will be provided 100% escort <u>at all times</u> when performing work at AEDC.

WEAPONS

It is a Federal Offense to introduce prohibited weapons at AEDC.

<u>PROHIBITIONS - Privately Owned Firearms, Explosives and Other Weapons</u>

- Introducing, transporting, using, or simply possessing ammunition, firearms, explosives, or other lethal weapons in the Mission Area (MA) or Arnold Village (AV), except when and where authorized (see "Hunting") **is prohibited.**
  - Possession includes not only having items on one's person, but also having items under one's control (in buildings/facilities, offices, vehicles, etc.)
  - Transporting is defined as having the personally owned weapon inside the vehicle you are operating.
- Civilian carry permits **are not recognized** within the Mission Area (MA), Arnold Village (AVA), Gossick Leadership Center (GLC), or any recreation area.
- Valid permits are recognized for carry while utilizing public accessible roadways. Possession/Transporting is permissible in accordance with state laws without a permit.
- Bows, arrows, and crossbows are governed by the same rules and regulations as firearms.
- Knives and other edged weapons are prohibited with the following exceptions: Pocket knives are allowed; hunting knives are subject to hunting regulations (see below); equipment items, such as a leatherman with a knife blade, used in day-to-day activities, are allowed; special cases evaluated and approved on an individual basis.
- Also Prohibited: Tasers, Air Guns (BB guns and pellet rifles), Throwing Stars, nun-chucks, Blackjacks, Saps, clubs, brass knuckles, or any other device intended to be used to strike a blow; razors, ice picks, or any like items concealed on one's person and/or not for business use; explosives including dynamite, C4, explosive powder, initiating explosives, squibs, detonating cord, blasting caps, detonators, fuses, fireworks, and any chemical compound, mixture, or device which the primary or common purpose is to function by explosion (black powder for muzzle loads—see "Hunting); stiletto, baton or nightstick, canister sprays, martial art weapons or electronic defense weapons.

HUNTING

- Personnel involved in hunting are bound by AAFB's Hunting Regulations, to include training, and must obtain an AAFB Hunting Permit. The POC for such activities is the AEDC Natural Resources Office, 454-2320.

TOBACCO REDUCTION POLICY

The work performed under this Subcontract shall be executed on-site at AEDC. In an effort to achieve a "Tobacco-Free" Air Force, and to provide a safe, healthy and comfortable environment, a Tobacco Reduction Policy is in effect during performance of this Subcontract. Subcontractor personnel shall only be permitted to smoke in designated smoking areas. The Subcontractor shall ensure all Subcontractor personnel adhere to this policy. Any questions related to this policy shall be referred to the Job Monitor for guidance.

VEHICLE USAGE & TRAFFIC LAWS AT AEDC

To operate a personally- or company-owned vehicle on the base, the following is required and must be readily available upon demand:

1. Possess a valid state driver's license.
2. Proof of ownership (title, state registration, bill of sale or lease agreement).
3. Proof of insurance.

All vehicle operators must comply with the rules of motor vehicle operation imposed by this Instruction, AFI 31-204, and the laws of the state of Tennessee. All personnel must maintain privately owned, registered vehicles in a safe operating condition.

1. Vehicle operators must ensure that passenger capacity is not exceeded when operating the vehicle.
2. Passengers must occupy seats intended for that purpose.
3. Passengers are not to attempt to enter or leave moving vehicles.
4. Operators are financially responsible for traffic fines resulting from vehicle law violations.
5. Operators are to make every effort to keep disabled vehicles from blocking traffic.
6. Operators of trucks or buses that become disabled must display flags, flares or reflectors, according to Tennessee Motor Vehicle Laws.
7. All personnel and their passengers operating privately own vehicles (POVs) on AEDC property will use seat belts.

The subcontractor and its employees shall comply with base traffic regulations and installation entry/exit security measures. All vehicles are subject to random vehicle inspections upon entry/exit and while on the Installation Security Services reservation. Entry/exit point inspections ensure the security, military fitness, or good order and discipline of the command, and may include an examination to locate and confiscate unlawful weapons and other contraband. These inspections may be random or mandatory for all.

Operators of POVs involved in an accident within the AEDC fenced MA or those roads restricted to the public, and so posted, take the following steps:

1. After caring for injured persons, immediately report the accident to the BDOC (454-5662).
2. Do not move the vehicle until permitted by the investigating officer, unless in the operator's opinion, it must be moved to avoid further accidents. (The extent of movement is limited to the absolute minimum.)
3. Under the provisions of Tennessee Code Annotated (TCA)., Section 55-12-104, persons must file or have filed a personal accident report with the Tennessee Department of Safety if:
   a. Involved in an automobile accident as an owner or driver involving death or injury.
   b. Damage to property was in excess of four hundred dollars ($400.00) to any person involved.
   c. To satisfy this requirement of TCA, Section 55-12-104 complete the State Form 0395.
   d. The report must be submitted to the Tennessee Department of Safety within 20 days from the accident.
   e. This report is required regardless of who was at fault and in addition to any report filed by an investigating officer.
   f. Failure to file a personal accident report with the Tennessee Department of Safety may result in the suspension of driver license and registrations or non-resident operating privileges of any person involved in the accident.
   g. When an accident occurs in a state other than Tennessee, information on required reports for that state must be obtained from the investigating officer. Installation Security Services investigates vehicle accidents occurring on AEDC or notifies other law enforcement agencies as appropriate.

The NAS project monitor will coordinate with affected building managers and Security Services Contractor (SSC) on all construction zone parking.

1. Parking is prohibited in any manner which:

   a. Obstructs a fire lane or is within 15-feet of any fire hydrant.
   b. Creates a safety hazard for personnel, facilities, or equipment.
   c. Obstructs traffic.
   d. Is on seeded areas and non-paved surfaces.
   e. Is within 10-feet of any building, structure, or equipment that does not have delineated lines designating authorized parking.
   f. Is on streets and roadways on AEDC except in areas specifically designated for parking.

Persons granted the privilege of operating a motor vehicle on a military installation in accordance with AFI 31-204, are deemed to have consented to a chemical test of their blood, breath, or urine, which determines their blood alcohol/drug content if they are cited or lawfully apprehended for any offense allegedly committed while they were under the influence of an intoxicating liquor/drug.

1. The test is incidental to a lawful apprehension and administered at the direction of the installation law enforcement official(s) having probable cause to believe a person was driving or was in the actual physical control of a motor vehicle on the installation while under the influence of an intoxicating liquor/drug.

2. Persons, who have died, are unconscious, or otherwise in a condition rendering them incapable of refusing, are deemed not to have withdrawn their consent.

3. The tests may be administered whether or not people are told that their failure to submit to or complete the test will result in the suspension of their privilege to operate a motor vehicle.

4. Any person granted the privilege of operating a motor vehicle on an installation in accordance with AFI 31-204 shall be deemed to have given his consent for the removal and temporary impoundment of the POV when it is parked illegally for unreasonable periods (24 hours), interfering with operations, creating a safety hazard, disabled by accident, left unattended in a restricted or Closed Area, or abandoned.

Cost of towing and storage, should a vehicle be moved or impounded, is the responsibility of the owner.

Subcontractors are responsible for securing private property. POVs are subject to inspections by the Government or other CSS at any time while on AAFB, NFAC Moffett Field, or AEDC - White Oak property

DELIVERIES

Delivery of subcontractor materials or equipment shall be made through Gate 2. Prior notification is required for materials delivery and any materials to be taken off AEDC.

POSTING, DISTRIBUTING, AND SOLICITING

Posting or distributing newspapers, magazines, handbills, posters, or notices on AEDC property without proper authorization is prohibited.

LABOR PROTESTS

If the subcontractor becomes a target of a labor protest while working on the installation, the subcontractor will be assigned a gate to enter and exit the MA, other than the main gate. All subcontractor employees will be directed to utilize the designated strike gate.

FORCE PROTECTION CONDITION (FPCON)

Subcontractor Monitors will ensure subcontractors are briefed and knowledgeable of and comply with FPCON requirements. FPCON is a Department of Defense (DoD) approved system standardizing DoD's identification of and recommended preventive actions and responses to terrorist threats against U.S. personnel and facilities. The system is the principal means for a commander to apply an operational decision on how to protect against terrorism and facilitates coordination among DoD Components and support for antiterrorism activities.

During FPCON changes (real-world and exercises), the subcontractor may be subject to various security reviews/checks and participate in exercises in conjunction with any DoD activity assigned. Any such security exercise shall be deemed a sovereign act of the government and shall not entitle subcontractor to an equitable adjustment in the price of this agreement.

1. The DoD FPCON consists of five progressive levels of increasing Anti-Terrorism protective measures. The implementing measures for each level are detailed in sections E4.4. and E4.5. The circumstances that apply and the purposes of each protective posture are as follows:
2. FPCON NORMAL: Applies when a general global threat of possible terrorist activity exists and warrants a routine security posture. At a minimum, access control will be conducted at all DoD installations and facilities.
3. FPCON ALPHA: Applies when there is an increased general threat of possible terrorist activity against personnel or facilities, and the nature and extent of the threat are unpredictable. ALPHA measures must be capable of being maintained indefinitely.
4. FPCON BRAVO: Applies when an increased or more predictable threat of terrorist activity exists. Sustaining BRAVO measures for a prolonged period may affect operational capability and military-civil relationships with local authorities.
5. FPCON CHARLIE: Applies when an incident occurs or intelligence is received indicating some form of terrorist action or targeting against personnel or facilities is likely. Prolonged implementation of CHARLIE measures may create hardship and affect the activities of the unit and its personnel.
6. FPCON DELTA: Applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is imminent. This FPCON is usually declared as a localized condition. FPCON DELTA measures are not intended to be sustained for an extended duration.

AUTOMATED INFORMATION SYSTEM (AIS) REQUIREMENTS

If subcontractor's employees require access to AEDC unclassified computer systems the following requirements apply:

1. Users must be a U.S. Citizen.
2. Users must successfully attain at least a Tier 1 Background Investigation.
3. Users must complete a DD Form 2875, System Authorization Access Request (SAAR), to request access.
4. Requestor must have a favorable National Agency Check with Inquiries.
5. Requestor must complete the DoD CyberSecurity Awareness Challenge.
6. Users bringing Portable Electronic Devices on base wanting to connect to AEDC computer systems/networks shall comply with established AEDC procedures, consult job monitor.

Users shall not connect any flash media based device to a government computer. Flash media devices are items such as thumb drives, cameras, and cell/smart phones. Also, note that even connecting a phone to a computer to charge will result in a violation.

TOOL CONTROL REQUIREMENTS FOR FOREIGN OBJECT AWARENESS AREAS

Tool Control Requirements to be used when working in Foreign Object Critical Awareness Areas:

1. A dispatchable consolidated tool kit (DCTK) is any tool kit that is not permanent to a Foreign Object (FO) Awareness or FO Critical Area that will be used by personnel to perform work in an FO Critical or Awareness Area.

2. A DCTK may include tools owned by the Government, AEDC contractors, subcontractors, and non-AEDC contractors and subcontractors including test customers.

3. A DCTK shall be utilized for the shortest period necessary to perform the work.

4. Each DCTK shall have a custodian assigned.

5. All tools, expendable tools, and consumables must be marked to identify the custodian and/or tool kit.

6. Each DCTK shall have a temporary Master Inventory List (MIL) of all tools, expendable tools, and consumables; and identifies the custodian.

7. Inspect DCTK daily, record inventory on AFMC Form 1771, and report inspection results as required by Area Supervisor, Technical POC, or Master Permit Issuer. Inventories must be accomplished and documented upon the first opening and last closing of every shift. (Form AFMC 1771may be downloaded at *nas-llc.us/terms-and-conditions),*

8. Lost tools must be immediately reported to the work permit issuing official or other work area responsible person.

9. If unmanned storage of DCTK is required, provide the following:
   a. Lockable storage security protection (gang box, job box, cabinet, room, vehicle compartment, etc.).
   b. Protection from weather or other potential physical harm.
   c. Marking outside of storage units with name of Custodian and work crew organization.

10. At the end of work assignment: perform a final inventory, and remove the DCTK from the FO Awareness or FO Critical Area.

REFERENCES AND FORMS

References
AAFB IDP 31-101, Arnold Air force Base Integrated Defense Plan, November 2018

Forms
AEDC Form 898, Contractor Clearance Request
AEDC Form 900, Contractor Employment Notice
DD Form 441, DoD Security Agreement
DD Form 254, DoD Contract Security Classification Specification
DD Form 2345, Military Critical Technical Data Agreement
DD Form 2875, System Authorization Access Request (SAAR)
AFMC Form 1771, Toolbox Inventory Record (Form may be downloaded at *nas-llc.us/terms-and-conditions)*

AEDC References and prescribed forms are available upon request.