

**BY ORDER OF THE COMMANDER  
AIR EDUCATION AND TRAINING  
COMMAND**

**AF INSTRUCTION 31-210**

**AIR EDUCATION AND TRAINING COMMAND  
Supplement 1**

**5 APRIL 2000**

**Security**



**THE AIR FORCE ANTITERRORISM/FORCE  
PROTECTION (AT/FP) PROGRAM  
STANDARDS**

---

**NOTICE:** This publication is available digitally on the HQ AETC Publishing WWW site at: <http://www.aetc.af.mil/im>. If you lack access, contact your Base Publishing Manager.

---

OPR: HQ AETC/SFPC (SMSgt R. Baliko)  
Supersedes AFI 31-210/AETC Sup 1,  
6 April 1998

Certified by: HQ AETC/SFP (Lt Col B. Detrick)  
Pages: 7  
Distribution: F

---

**AFI 31-210, 1 August 1999, is supplemented as follows:**

**NOTE:** Maintain and dispose of records created as a result of processes prescribed in this publication in accordance with AFMAN 37-139, Records Disposition Schedule.

**SUMMARY OF REVISIONS**

**This publication has been substantially revised and must be completely reviewed.**

3.1.11. Each HQ AETC directorate and staff agency will implement an AT program and designate an AT program manager in writing. Each directorate will provide a copy of a memorandum of appointment of an AT officer or NCO to HQ AETC/SFPC. (Security managers may be appointed this additional duty.) The 12 FTW Installation Security Plan (ISP) will serve as the guideline for AT procedures.

3.1.12. (Added) In AETC, responsibilities for the AT program and the focal point for AT matters is HQ AETC/SF (through HQ AETC/SFPC). This focal point will:

3.1.12.1. Coordinate AT policy and guidance with HQ USAF/XOF.

3.1.12.2. Disseminate AT policy and guidance to AETC bases and associated units.

3.1.12.3. Coordinate on requests from AETC bases for training quotas through HQ AETC/SFXT for unique course requirements pertaining to the AT program.

3.1.12.4. Coordinate requests for exceptions to vehicle marking and painting requirements stemming from a terrorist threat through HQ AETC/LG.

3.1.12.5. Evaluate base AT plans and programs during staff assistance visits and vulnerability assessments.

3.1.12.6. Allocate funding provided by the Air Force Financial Management Board (FMB) to AETC bases for security enhancement and AT projects.

3.1.12.7. Train HQ AETC directorate and staff agency AT officers and NCOs on basic responsibilities unique to headquarters functions.

3.1.12.8. Consider providing a command representative to accompany Defense Threat Reduction Agency (that is, Joint Staff Integrated Vulnerability Assessment [JSIVA]) and Air Force Security Forces Center teams (AF VAT) during vulnerability assessments of AETC bases.

3.2.3. Each AETC base will update its installation security and/or AT/FP plan to reflect the requirements of the basic paragraph. Each base will update and publish the plan within 120 days of the release of a MAJCOM supplement. A copy of the plan will be sent to HQ AETC/SFPC. In addition, each AETC base will develop a written barrier plan for effective employment of barriers (paragraph 3.5.2, this supplement). This plan may be an annex to the base's installation security plan. The plan must be tested through exercises conducted annually by the base exercise evaluation team (BEET), and consideration must be given to high occupancy buildings and approaches to the installation. Barriers used must be connected with steel cables to prevent them from being moved by vehicles. If cost is a factor, there are several barriers that can be procured or manufactured. Whichever barrier type is chosen, the AT officer or NCO must ensure the barriers are heavy enough to prevent vehicles from crashing through them. See Attachment 6 (Added), this supplement, for installation standards for barriers, fencing, etc.

3.3.3. Headquarters Air Force Recruiting Service (HQ AFRS), Headquarters Air Force Officer Accession and Training Schools (HQ AFOATS), and HQ AETC directorates will comply with training requirements in the basic AFI. **NOTE:** The AFOATS designee for AT will coordinate the development of terrorist awareness and countermeasures training for permanent party personnel assigned to AFOATS field units.

3.3.4. Each installation's chief of security forces (CSF) will serve as the focal point for the installation's AT program as follows:

3.3.4.1. The security forces AT officer or NCO will continuously coordinate with the local Air Force Office of Special Investigations (AFOSI) to obtain terrorist threat information and inform the installation commander of changes in the level of threat to base personnel and/or facilities.

3.3.4.2. Installations will establish a threat working group to address AT program matters. The threat working group should include representatives from security forces, civil engineer readiness, medical readiness, intelligence, and AFOSI for help in developing AT requirements. The local AFOSI detachment will conduct an annual threat assessment of the installation.

3.3.4.3. Using the DSHARPP concept, either the AFOSI or the threat working group will identify high-risk personnel or facilities requiring special attention. (The acronym DSHARPP stands for **D**emographics, **S**ymbolism, **H**istory, **A**ccessibility, **R**ecognizability, **P**roximity, and **P**opulation.) Realistic exercises based on the local threat and current threat condition (THREATCON) must be performed at least semiannually.

3.3.4.4. Commander's access channels, base bulletins, and base-wide e-mail can be used to disseminate threat information. Personnel on an installation (to include family members) should be made aware of what actions they are required to take while in any particular THREATCON. The JSIVA and AF VATs will randomly ask personnel (contractors, civil service employees, TDY personnel, students, visitors, and active duty military) on the installations they visit the following questions: What is the current threat condition, why was this condition implemented, and what actions need to be done for the current threat condition?

3.3.4.5. To inform personnel of the current THREATCON, use the following AETC visual aids (AETCVA), as applicable: AETCVA 31-1, **THREATCON Alpha** (tan); AETCVA 31-2, **THREATCON Bravo** (blue); AETCVA 31-3, **THREATCON Charlie** (yellow); or AETCVA 31-4, **THREATCON Delta** (red). These visual aids are available electronically on CD-ROMs and the official AETC publications web site. When printing these visual aids, they *must* be printed on the applicable color paper. Therefore, units will ensure they have an adequate supply of the colored paper.

3.5.2. The Air Force Security Forces Center has developed a template for installation AT plan development. HQ AETC/SFPC will obtain and distribute these templates to all active duty and Air National Guard bases under AETC's control. All AT plans will have a comprehensive barrier and enclave plan to protect personnel on the installation. Plans must address barrier placement, types to be used, coordination in establishing barriers around high-risk facilities, unused gates, installation entry points, and straight-line access to facilities. The barrier and enclave plan must be exercised semiannually. When designing and landscaping buildings or areas, consider using bollards and natural barriers such as trees, hedgerows, and berms.

3.6.2. AETC bases will be assessed by either the JSIVA, AF VAT, or HQ AETC's vulnerability assessment teams (VAT). HQ AETC/SF will coordinate all VAT visits with HQ AETC/IGIX (Gatekeepers). These teams will include functionals from intelligence, infrastructure engineer, communications, structural engineer, threat assessment, operational readiness, physical security, and force protection. This assessment is a "snapshot in time" of the installation's ability to detect and deter a potential domestic or international terrorist attack; it is not an inspection with findings. The report will be classified Secret and should be delivered to the installation commander within 60 days of the conclusion of the assessment. The report should be made available to the installation threat working group and be used for planning purposes only. It does not need to be answered.

3.13.1.4. Installation commanders will ensure a minimum of three random antiterrorism measures (RAM) are conducted on the installation daily. RAM is not a *security forces* program only. The entire installation must establish a RAM program and ensure its implementation is properly documented. **NOTE:** A possible documentation source would be the security forces blotter. The security forces normally conduct one RAM every 8 hours. Other installation units conducting a RAM could call the start time, duration, and type of RAM being implemented into the security forces desk to be recorded in the blotter. This would add at least two additional entries to the security forces desk blotter and provide the permanent record of RAM implementation required by this AFI. Another documentation source would be an electronic events log maintained by the wing command post.

3.15.1. The installation barrier and enclave plan may be part of this section.

3.15.6. (Added) The installation plans branch will ensure all wing plans, such as installation security and base recovery, are comprehensive and include areas such as weapons of mass destruction and biological and chemical attack as well as peacetime disasters. These could include events such as a train derailment or the crash of a tanker truck on a highway running adjacent to the installation.

3.18. All military construction (MILCON) projects should be reviewed by security forces and civil engineers for compliance with DoD-mandated construction AT standards. Security forces should be included in all planning meetings for the entire MILCON project. Review all current DoD AT construction standards for incorporation into new MILCON projects.

3.26. The installation security council should evaluate the need to install duress systems to safeguard high-risk personnel. High-risk personnel must be identified by position in the installation security plan.

**3.34. AT Awareness Initiatives.** See Attachment 7 (Added), this supplement, for AT awareness initiatives.

A3.2.2. Use AETCVA 31-1 to announce an exercise or actual THREATCON Alpha.

A3.3. Use AETCVA 31-2 to announce an exercise or actual THREATCON Bravo.

A3.4. Use AETCVA 31-3 to announce an exercise or actual THREATCON Charlie.

A3.5. Use AETCVA 31-4 to announce an exercise or actual THREATCON Delta.

**Attachment 6 (Added)****INSTALLATION STANDARDS FOR BARRIERS AND FENCING****A6.1. Barriers and Installation Gates:**

**A6.1.1.** Installations should be equipped with a movable barrier capability at all installation gates. Installations not so equipped must identify their requirements to HQ AETC/SFX for programming action.

**A6.1.2.** Installation gates should have the capability of being secured (closed) to both incoming and outgoing traffic. Routinely manned installation entry gates will have either electronic or manually closing iron gates (anchored at both ends of the gate) to keep vehicles attempting to ram the gate from gaining access to or exiting from the installation. Portable barriers may be used at installation gates as a blocking tool if they are cabled together with at least 3/4-inch steel cable.

**A6.1.3.** Portable barriers should be used in conjunction with other tools, such as bollards. Bollards are recommended for gates because they can be easily installed and removed to be stored near the gate's location.

**A6.1.4.** Fill bollards with concrete at least one-half the length of the exposed bollard above ground and the entire length beneath ground. This will prevent vehicles from defeating the bollard by ramming them. Concrete-filled bollards can be installed and removed by as few as two people. All installation entry points with at least 50 feet of acceleration area towards the gate will employ a bollard serpentine to slow a vehicle's approach.

**A6.1.5.** Bollards are also excellent barriers for temporarily closing roadways or parking lots. All unmanned installation gates can and should be secured by jersey-style concrete barriers at least one-barrier length past each side of the gate. Consult HQ AETC/SFPC for guidance on effective barrier employment.

**A6.2. Installation Perimeter Fencing:**

**A6.2.1.** The standard for AETC installation perimeter fencing is chain-link or metal woven fence, at least 6-feet high and preferably with outriggers. The fence will be anchored with vertical supports at least 4 feet apart or with a 1/4-inch steel cable anchoring the fence line no more than 18 inches above ground level. This will prevent a vehicle from defeating the fence line.

**A6.2.2.** The fence needs to be checked periodically to prevent vegetation from overgrowing and erosion from causing gaps under the fence line.

**A6.2.3.** Installation warning signs will be placed along the fence line at regular intervals, indicating the presence of a military installation. Signs should be kept in good repair. Standards for installation fences can be found in DoD O-2000.12-H, Chapter 9, *Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence*.

**Attachment 7 (Added)****AT AWARENESS INITIATIVES**

**A7.1. Overview.** The following paragraphs contain general initiatives for various locations in which persons may find themselves or their family members. The intent is to provide initiatives to help develop pamphlets and public awareness at AETC installations. While these initiatives were developed as part of executive protection for senior-ranking personnel, they can be applied to family members as well.

**A7.2. At Home:**

**A7.2.1.** Become familiar with delivery and commercial service personnel. (for example, mail carriers, newspaper delivery, electric, water, and gas meter readers). Teach family members how to properly use the "911" or other emergency notification systems.

**A7.2.2.** Consider a family code, similar to a covert duress code, to be given on an as-needed basis. That way, family members will know who they are dealing with when parents or people they recognize aren't able to meet them or pick them up from functions. Teach young family members to say "no" to strangers and to immediately report any encounter of strangers to you.

**A7.2.3.** Teach family members how to detect potential letter or package bombs.

**A7.2.4.** Exercise on varying schedules; avoiding similar routes and distances while jogging or bicycling.

**A7.2.5.** Ensure contract work on your residence is known to all occupants.

**A7.2.6.** Before entering your vehicle, examine it for improvised explosive devices, especially during increased THREATCONs.

**A7.2.7.** Before opening the door, identify persons on the other side of the front door by looking through a "peephole."

**A7.2.8.** Do not make a habit of leaving keys to your residence in hiding places. An intruder knows exactly where to look. Leave an extra key with the manager or a trusted neighbor, if necessary.

**A7.2.9.** If you use an answering machine, listen to the message recorded on it. Never reveal a name, phone number, or residence address.

**A7.2.10.** Teach family members to insist on proper identification from strangers attempting to enter your residence.

**A7.2.11.** Do not permit your trash to become a source of information about you or your family.

**A7.3. Traveling To and From Home:**

**A7.3.1.** Avoid routines with recurring timetables; do not allow others to predict your movements. Keep vehicles locked and windows rolled up all the way when leaving vehicles unattended, especially while traveling. Vehicles parked on a military installation should also be locked and the windows rolled up.

**A7.3.2.** Do not make en route stops predictable or frequent. Make a habit of refueling when the gas gauge reads just over 50 percent. Try to avoid alleys, poorly lit thoroughfares, and traffic congestion. Keep your vehicle in good working order. Park it in the most secure and well lit area possible.

**A7.3.3.** If you believe you are being followed, do not go to your residence. Proceed to the nearest police station, fire station, or populated area and seek assistance. If possible, record the make, license number, color, and occupants of the vehicle.

**A7.4. Going on Vacation:**

**A7.4.1.** Before going on vacation, consider stopping regular deliveries and making arrangements for your lawn to be taken care of. Purchase and use electric timers to activate lights, TVs, radios, etc.

**A7.4.2.** Remember, most people do not go a week or two without generating trash. Have a neighbor place the trash in your can and place the can on the curb for trash pickup. Invite a trusted friend to routinely occupy your residence and rearrange drapes and blinds.

**A7.4.3.** Do not set a pattern if you stop at a vacation site. If on vacation in a foreign country, know how to contact local law enforcement and other emergency agencies. Do not advertise the fact that you or your family members are associated with the military.

**A7.5. When Staying at a Hotel:**

**A7.5.1.** Avoid accommodations with distinctively American names, but use DoD facilities as much as possible.

**A7.5.2.** Choose an inside hotel room and avoid taking street-level or terrace-level rooms with direct access to the hotel grounds or stairwells. If this cannot be done, sleep away from street-side windows.

**A7.5.3.** Answer the telephone with "hello," never a name and rank. Look before you exit your room and keep your key with you at all times. Do not give your information, such as name, room number, phone number, etc., to strangers. Leave a light on when you are not in the room.

**A7.5.4.** Do not accept packages or unexpected mail in your room. Instead, have all mail sent to the receiving desk. Retain positive control over your luggage on arrival at the hotel lobby.

RICHARD K. ELDARD, Colonel, USAF  
Director of Security Forces