

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



AF INSTRUCTION 10-245

**AIR EDUCATION AND TRAINING COMMAND
Supplement 1**

14 SEPTEMBER 2004

Operations

AIR FORCE ANTITERRORISM (AT) STANDARDS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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/SFP (Capt Joseph D'Amico)
Supersedes AFI 31-210/AETC Sup 1, 5 April 2000

Certified by: HQ AETC/SF (Lt Col Stephen Priore)
Pages: 22
Distribution: F

AFI 10-245, 21 June 2002, is supplemented as follows:

This publication does not apply to the Air National Guard or the Air Force Reserve Command. Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 37-123, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) (available at <https://webrims.amc.af.mil>). The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed. This revision updates the membership requirement for the force protection working group (FPWG) and how often it must meet (paragraph 2.1.1.14.1 [Added][AETC]); requires random antiterrorism measures (RAMs), barrier plan implementation and scope of AT training be added to the AT plan (paragraph 2.1.1.14.1.1 [Added][AETC]); requires installations to review lessons learned and close open items (paragraph 2.1.1.14.1.2 [Added][AETC]); requires installations to review memorandums of agreement and/or understanding, and review open installation vulnerabilities and mitigation progress, AT construction projects, force protection (FP) upgrades to existing facilities, and AT funding (paragraph 2.1.1.14.1.3 [Added][AETC]); breaks down the HQ AETC FP structure (paragraphs 2.1.1.14.2., 2.1.1.14.2.1., 2.1.1.14.2.2 [Added][AETC]); identifies HQ AETC/SFP as the focal point for AT matters (paragraph 2.1.1.14.3 [Added][AETC]); makes AT representatives or unit training managers responsible for tracking Level I AT training status for personnel assigned their directorate or staff agency (paragraph 2.1.1.14.3.5.1 [Added][AETC]); adds that AT representatives will attend FPWG meetings (paragraph 2.1.1.14.3.5.2 [Added][AETC]); assigns HQ AETC/SF or designated representative as the chair for the Force Protection Requirements Committee (FPRC) (paragraph 2.2.1.4); provides guidance to include contractor personnel into installation AT program (paragraph 2.5.2); adds installation antiterrorism officer (ATO) requirements (paragraph 2.6.1); adds unit

level AT representative requirements (paragraph 2.6.1.1 [Added][AETC]); requires installation ATOs to forward a copy of appointment letters to HQ AETC/SFP (paragraph 2.6.1.2 [Added][AETC]); requires installation ATOs or their AT designee to be level II trained and be a member of the base exercise evaluation team (EET) (paragraph 2.6.4.5); requires installation ATOs to maintain AT program continuity books (paragraph 2.6.4.13 [Added][AETC]); provides guidance on how to disseminate threat information (paragraph 2.9.4); encourages tenant units to develop their own specific security plans that complement the AT plan (paragraph 2.14.2.1 [Added] [AETC]); provides plan guidance for the installation plans branch (paragraph 2.14.3); provides guidance for the installation barrier plan (paragraph 2.16.3.1 [Added] [AETC]); requires semiannual exercises that test reporting procedures, implementation of each force protection condition (FPCON), full implementation of the installation barrier plan, mass notification procedures, and evaluate reporting of plans to evaluate traffic flows, and unit support of staggered reporting plans (paragraph 2.19.2 [Added][AETC]); identifies HQ level I training requirements (paragraph 2.22.1); provides local vulnerability assessment (VA) guidance (paragraph 2.26.2.1.1.1 [Added][AETC]); it provides local VA reporting requirements (paragraph 2.26.2); directs installations conducting local VAs to use the mission, symbolism, history, accessibility, recognizably, proximity, and population (MSHARPP) to identify high risk personnel and facilities (paragraph 2.26.2.1); and it identifies requirements for loading vulnerabilities into the Vulnerability Assessment Management Program (VAMP) (paragraph 2.26.13).

2.1.1.14.1. (Added)(AETC) In accordance with the basic AFI, each AETC installation will establish a force protection working group (FPWG) to provide oversight of installation plans and mitigation of installation vulnerabilities. FPWG membership will include representatives from SFS, CES, CS, MDG, SVS, wing plans, MSS, OG, MSG (or SPTG), DOYI, JA, CONS, CPTS, PA, SE, AFOSI, and the installation antiterrorism officer (ATO). The FPWG will identify and define installation AT requirements. AETC installation FPWGs will include representatives from all tenant units. The FPWG will meet at least quarterly, and meeting minutes will be approved by the installation commander. File meeting minutes with the installation ATO for 2 years to track open items. The FPWG will report the status of the installation AT program during each meeting of the installation security council, to include:

2.1.1.14.1.1. (Added)(AETC) Effectiveness of the installation AT plan, including unit-level random antiterrorism measure (RAM) efforts, barrier plan implementation, and scope of AT training.

2.1.1.14.1.2. (Added)(AETC) AT lessons learned and efforts to close open items.

2.1.1.14.1.3. (Added)(AETC) Base consequence management preparedness. Review memorandums of agreement (MOA) and/or understanding (MOU) if using local community assets to supplement installation capabilities. Review open installation vulnerabilities and mitigation progress, AT construction projects, FP upgrades to existing facilities, and AT funding.

2.1.1.14.2. (Added)(AETC) The HQ AETC FP structure is broken into two groups: the FPWG and threat working group (TWG).

2.1.1.14.2.1. (Added)(AETC) HQ AETC FPWG composition, duties and responsibilities are outlined in Attachment 9 (Added)(AETC).

2.1.1.14.2.2. (Added)(AETC) HQ AETC TWG composition, duties and responsibilities are outlined in Attachment 10 (Added)(AETC).

2.1.1.14.3. (Added)(AETC) In AETC, responsibility for the AT program and the focal point for AT matters is HQ AETC/SF (through HQ AETC/SFP). Each HQ AETC directorate and staff agency will implement an AT program, and designate an AT representative in writing. Each directorate will provide a copy of a memorandum of appointment of an AT program manager to HQ AETC/SFP (directorate FPWG representatives or security managers may be appointed for this additional duty). The 12 FTW Installation

Security Plan (ISP) (contact HQ AETC/SFP) will serve as the guideline for HQ AETC AT procedures. HQ AETC/SF will:

- 2.1.1.14.3.1. (Added)(AETC) Coordinate AT policy and guidance with HQ USAF/XOF.
- 2.1.1.14.3.2. (Added)(AETC) Disseminate AT policy and guidance to AETC bases and associated units.
- 2.1.1.14.3.3. (Added)(AETC) Coordinate on requests from AETC bases for training quotas through HQ AETC/SFXT for unique course requirements pertaining to the AT program.
- 2.1.1.14.3.4. (Added)(AETC) Evaluate base AT plans and programs during staff assistance visits and vulnerability assessments.
- 2.1.1.14.3.5. (Added)(AETC) Train HQ AETC directorate and staff agency AT representatives on basic responsibilities unique to headquarters functions.
 - 2.1.1.14.3.5.1. (Added)(AETC) AT representatives or unit training managers are responsible for tracking Level I AT training status for personnel assigned to their directorate/staff agency.
 - 2.1.1.14.3.5.2. (Added)(AETC) AT representatives will attend FPWG meetings.
- 2.1.1.14.3.6. (Added)(AETC) 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. Encourage other functional representatives from the FPWG to accompany VA teams.
- 2.2.1.4. HQ AETC/SF or designated representative chairs the Force Protection Requirements Committee (FPRC), which is responsible for evaluating and validating AT funding requests from AETC installations. The FPRC, through the AETC corporate process, allocates funding provided by the Air Force Council to AETC installations for security enhancement and AT projects. The FPRC should utilize data generated by the Vulnerability Assessment Management Program (VAMP) to prioritize and review AT projects for funding.
 - 2.2.1.4.1. HQ AETC/SFX will coordinate with AETC installations to gather program objective memorandum requirements for AETC installations.
 - 2.2.1.4.2. Unless otherwise specified by HQ AETC/SFP, AETC installations will forward Combating Terrorism Readiness Initiative Fund (CbTRIF) requests to HQ AETC/SFP no later than 15 January and 15 July annually. CbTRIF submissions will be generated using the VAMP.
 - 2.2.1.4.2.2. (Added)(AETC) The HQ AETC FPWG will review, edit, and prioritize AETC CbTRIF packages for submission to the appropriate combatant commanders.
- 2.3.4.1. Document this review via memorandum for record and maintain on file with the installation ATO.
- 2.3.4.2. Installation commanders will establish an active public affairs program to combat terrorism. Public affairs personnel will work closely with the installation ATO to increase AT awareness, and dispel rumors and misinformation by providing appropriate and timely information to the base populace using installation media/information resources (commander's calls, base newspaper, and commander's access channel). The installation ATO may also use other venues for disseminating information to the installation populace such as the base intranet and base bulletin.
- 2.5.2. In order to be effective, an AT program must reach all personnel working on the installation, to include contractor personnel. Contractors working on the installation should participate with the installation populace in AT awareness education (consistent with contractual requirements), USAF Eagle Eyes program (managed by AFOSI), RAMs, and AT/FP security measures implementation. The contracting office should work closely with security forces and the installation ATO (paragraph 2.17.3 of this supplement) to ensure

AT/FP security requirements, as well as contractor participation in installation AT/FP exercises, are included in contracts.

2.6.1. In accordance with the basic instruction, all AETC installation commanders will appoint a wing level AT officer (ATO) in the grade of E-6 (or civilian equivalent) or above and an alternate ATO. The ATO is a key member of the installation commander's staff, and is the focal point for the installation AT program. As an advisor to the installation commander, the ATO position will be organized and supervised on the wing staff. Due to the complexity and scope of ATO responsibilities, individuals appointed as the installation ATO should not be tasked with this responsibility as an additional duty.

2.6.1.1. (Added)(AETC) The commander of each unit/tenant organization on the installation will appoint in writing a unit level AT representative to coordinate unit/tenant organization participation in the installation AT program with the installation ATO (unit security managers may be appointed this additional duty).

2.6.1.2. (Added)(AETC) AETC installations will forward a copy of their ATO appointment letter to HQ AETC/SFP, 1851 First Street East, Suite 2, Randolph AFB TX 78150-4316. Include in this letter the date graduated from the ATO Level II Course, NIPR and SIPRNET e-mail addresses, cell phone or pager number, and duty phone numbers.

2.6.4.1. The local Air Force Office of Special Investigations (AFOSI) and wing intelligence flight (if applicable) will continuously coordinate with the installation ATO to provide timely terrorist threat information to the installation commander, and inform the commander of changes in the level of threat to base personnel and/or facilities.

2.6.4.5. AETC installation ATOs, or as a minimum their AT designee (AT Level II trained), will be members of the base exercise evaluation team (EET), and will be responsible for drafting and conducting AT exercise scenarios. In addition to wing level exercises, the installation ATO will conduct periodic, random AT exercises to test AT awareness at the unit/tenant organization level.

2.6.4.13. (Added)(AETC) In order to maintain standardization and consistency of AT programs across AETC installations, the installation ATOs and unit AT representatives will maintain AT/FP program continuity books (or folders). Continuity book requirements are listed in Attachment 11 (Added)(AETC) to this supplement. The installation ATO will inspect the continuity books annually. ATOs will use the installation ATO AT/FP POC checklist at Attachment 12 (Added)(AETC) to this supplement in order to assist with meeting program requirements.

2.9.4. Commander's access channels, base bulletins, and base-wide e-mail can be used to disseminate threat information. To inform personnel of the current FPCON (actual or exercise), use the following AETC visual aids (AETCVA), as applicable: AETCVA 31-1, *FPCON Alpha* (tan); AETCVA 31-2, *FPCON Bravo* (blue); AETCVA 31-3, *FPCON Charlie* (yellow); or AETCVA 31-4, *FPCON Delta* (red). These visual aids are available electronically on CD-ROMs and on the official AETC publications web site. When printing these visual aids, they must be printed on the appropriate color paper. Therefore, units will ensure they have an adequate supply of the colored paper. Magnetic signs and window clings are authorized.

2.13.2.1. Installation commanders may implement higher FPCONs based on local conditions. Downward directed FPCON changes will come through the AETC crisis action team (CAT). Tenants will comply with the host installation FPCON, regardless of the FPCON declared by their parent command. Tenants may increase security at their respective facilities through the use of an expanded RAM program, coordinating with the host security organization. There will only be one FPCON on AETC installations with the final determination made by the installation commander.

2.13.4. Installation commanders will ensure RAMs are conducted in accordance with the interim change to Air Force Protection Conditions message. The RAM program is an installation program, involving ALL

units and personnel. AETC installation commanders are responsible for developing and implementing a RAM program and documentation procedures to ensure RAMs are conducted and reported to the ATO. **NOTE:** For example, a possible documentation source could be the wing command post events log. The security forces normally conduct two RAMs per shift, as a minimum, and record it in the security forces blotter. Other installation units conducting daily RAMs should call the start time, duration, and type of RAM implemented into the command post to be recorded in the events log. Another means of tracking RAMs is through e-mail, and an electronic database maintained by the installation ATO. Units conducting RAMs would e-mail date, time, and RAM conducted to the ATO, who in-turn would record it on an electronic database. Additionally, record RAMs conducted at the unit level in Section 4 of the AT/FP Program Continuity Book (Attachment 11 [Added][AETC], this supplement). This provides the installation ATO documentation required to monitor, track, and analyze RAM implementation efforts.

2.14.2. 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. Send a copy of the plan to HQ AETC/SFP. Additionally, each AETC base will develop a written barrier plan for effective employment of barriers (paragraph 2.16.3 this supplement). This plan may be an annex to the base installation security plan, or it may be a stand-alone plan. The plan must be tested through exercises conducted annually by the base EET. When selecting a vulnerability to test, consider high occupancy buildings and high-speed approaches to the installation.

2.14.2.1. (Added)(AETC) Encourage tenant units to develop their own specific security plans that complement ISP/AT plan.

2.14.2.2. (Added)(AETC) Include tenant units in installation AT planning.

2.14.3. 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, plus 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. The ISP/AT plan needs to reflect AT guidance for public events such as air shows, graduations, open houses, and other mass gatherings.

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

2.16.3. All AT plans will have a comprehensive barrier/bollard and enclave plan to protect personnel on the installation. Plans must address barrier/bollard placement around high-risk facilities, unused gates, installation entry points, straight-line access to facilities, and types of barriers/bollards to be used. The barrier/bollard and enclave plan must be exercised semiannually.

2.16.3.1. (Added)(AETC) When designing and landscaping buildings or areas, requirements of UFC 4-010-01, *DoD Minimum Antiterrorism Standards for Buildings*, and UFC 4-010-02, *DoD Minimum Antiterrorism Standoff Distances for Buildings* (contact installation CE for UFCs), shall be met. Using natural barriers eliminates the need for expensive and cumbersome artificial barriers, as well as being more aesthetically pleasing. When barriers/bollards are used, they must be connected with steel cables (where possible) to prevent them from being moved by vehicles. If cost is a factor, there are several barrier designs that can be procured or manufactured. Whichever barrier/bollard type is chosen, the installation ATO must ensure the barriers/bollards are heavy enough to prevent vehicles from crashing through them. See Attachment 13 (Added)(AETC) (this supplement) for installation standards for barriers/bollards, fencing, etc.

2.16.3.2. (Added)(AETC) Implement a robust barrier plan to control, deny, impede, and discourage access to the installation. The installation barrier plan must be a living document that is refined consistent with emerging threats. Include key facilities on the installation in the plan. The barrier plan must also address the types, storage, movement, and placement of barriers. Any changes to the published barrier plans must be fully coordinated with CES for the purchase, storage, and deployment of barriers.

2.17.3. The base contracting officer shall ensure a process is in place to conduct criminal background checks prior to employment. Contracting will ensure statements of work include security and FP provisions designed to ensure contractor compliance with the implementation of higher FPCONs, including subcontractor compliance.

2.17.4. Visitors and delivery vehicle operators applying for a pass or providing a delivery to the installation should have their license plates and driver's license checked for outstanding warrants. Additionally, the industrial/contractor gate should have a computer system installed to provide, at a minimum, automated lists to ensure quick and efficient processing of personnel requiring entry. Such a capability will enable the controller to track changes in contractor authority lists, and the numerous subcontractors that are employed for a given project.

2.17.6. (Added)(AETC) Over-watch, both lethal and nonlethal, must be addressed in advance in the base AT plan. Prior to employing an over-watch position, the staff judge advocate must review and approve rules of engagement (ROE). Whenever an over-watch position is employed, the position must have both nonlethal and lethal means of denying unauthorized entry, and must be positioned far enough away to monitor traffic, and have enough time to react, both nonlethally and lethally to unauthorized vehicles. Nonlethal means include, but are not limited to, tire deflation devices and/or a blocking vehicle. This may be accomplished by providing sufficient distance to react to a moving vehicle, or by using devices such as speed bumps, rumble strips, or barriers. If lethal force is an option, a formal operational risk management (ORM) review must be accomplished addressing, at minimum, rules of engagement, fields of fire, and potential for fratricide incidents. Communication between the over-watch position and installation entry controllers is paramount. Preestablished signals (between the entry controller and over-watch position) must be in place to ensure the over-watch position clearly understands when a vehicle needs to be stopped, and if lethal or nonlethal measures must be taken. The position must be employed in a (chokepoint) fashion, preventing vehicles from maneuvering around mitigating measures.

2.19.2. (Added)(AETC) Perform realistic exercises based on the local threat and current FPCON at least semiannually. Exercise and evaluate AT awareness, terrorist use of weapons of mass destruction (WMD), and the installation AT plan. Use international and domestic terrorist information to build realistic exercise scenarios. Where possible, include state, local, and federal authorities in exercises to increase realism. The scenarios may meet multiple requirements for Air Force exercises (HAZMAT, mass casualty, etc.) to meet various AFI requirements. The installation EET will document each exercise, providing a critique with findings, observations, and lessons learned. The installation FPWG is responsible for tracking exercise findings, and documenting actions taken to mitigate shortfalls and vulnerabilities to improve AT/FP processes. Properly documented real world scenarios may satisfy portions of this requirement. Exercises should, as a minimum, exercise measures and actions for FPCON Charlie, and must include:

2.19.2.1. (Added)(AETC) Indications of surveillance on and off base to test reporting procedures.

2.19.2.2. (Added)(AETC) Implementation of each FPCON with enough time spent in each FPCON to fully evaluate effectiveness of measures employed in response to the threat.

2.19.2.3. (Added)(AETC) Full implementation of the installation barrier plan.

2.19.2.4. (Added)(AETC) Mass notification procedures.

2.19.2.5. (Added)(AETC) Evaluate reporting plans to evaluate traffic flow and unit support of staggered reporting plans.

2.22.1. 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 ensure Level I AT (terrorist awareness and

countermeasures training) is provided for permanent party personnel assigned to AFOATS field units and officer accession trainees, via a qualified Level I AT awareness instructor, or computer-based training and/or distance learning.

2.22.6.3. AETC installations will report all personnel that arrive on station without Level I AT on a quarterly basis. Send reports to HQ AETC/SFP no later than 10 January, 10 April, 10 July, and 10 October. Provide all information as required by basic AFI. (RCS: HAF-SFC(AR)0126, Training Reports for Antiterrorism Level I and Level II Training)

2.24.9.1. HQ AETC/SF is the OPR for AT Level III training, and provides the required training during the AETC Squadron Commander's Course.

2.24.9.2. AT Level III instructors should be Level II course graduates, and have either installation-level ATO experience or AT instructor experience.

2.24.9.3. Installation ATOs will provide AT Level III briefings to any commanders who arrive on station without documented AT Level III training. HQ AETC/SFP will provide the standardized Level III curriculum slides to installation ATOs upon request to conduct the training.

2.26.2. AETC bases will be assessed by JSIVA, AF, or HQ AETC vulnerability assessment teams (VAT). HQ AETC/SF will coordinate all VAT visits with HQ AETC/IGIX (Gatekeepers). The vulnerability assessment (VA) report is classified in accordance with the Defense Threat Reduction Agency (DTRA) Force Protection Security Classification Guide, and will be delivered to the installation commander within 60 days of the conclusion of the assessment. The report should be made available to the installation FPWG and TWG, and should be used for planning purposes only. The report does not need to be answered.

2.26.2.1.1. When scheduling local VAs, ensure they are conducted within 12 months of the previous VA, whether a local or higher headquarters assessment. For example, if an installation received a higher headquarters assessment in May of 2003, it would need to conduct a local VA no later than May of 2004, and then no later than May 2005. Accordingly, HQ AETC/SFP will schedule the next higher headquarters assessment no later than May 2006.

2.26.2.1.2. (Added)(AETC) Installations will use the AFSFC antiterrorism VA guidelines when conducting local VAs. Forward a copy of the completed report to HQ AETC/SFP within 60 days of completion of the assessment.

2.26.2.1.3. (Added)(AETC) Units will provide HQ AETC/SFP a copy of any local VAs and update in VAMP within 10 days of report approval by the wing commander.

2.26.2.1. Using the mission, symbolism, history, accessibility, recognizability, proximity, and population (MSHARPP) concept, the local VA will identify high-risk personnel or facilities requiring special attention. See Attachment 14 (Added)(AETC) for further information on MSHARPP.

2.26.2.1.1. For tracking purposes, AETC installations will maintain the two most recent VA reports on file.

2.26.10.1. Submit Force Protection Integrated Support Team (FIST) support requests to HQ AETC/SFP, who will coordinate the request and send to HQ AFSFC/SFP.

2.26.12. The AETC VAMP administrator is HQ AETC/SF (SFP).

2.26.13. Vulnerabilities identified during local VAs will be entered into VAMP no later than 30 duty days following completion of the final report. Forward all vulnerabilities identified during VAs to the Installation Readiness Board, and address in accordance with AFI 10-2501, *Full Spectrum Threat Response (FSTR) Planning and Operations*.

2.28. DoD Standard 28 – Construction Considerations. All military construction (MILCON) projects will be reviewed by the installation ATO and civil engineers for compliance with DoD-mandated construction AT standards. The installation ATO 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.

2.28.2. The installation ATO, planners, and engineers should attend the Security Engineering Course. Consider sending 1-2 engineers, and the installation ATO.

2.28.2.1. Use AT planner software to provide technical input for decisions regarding barrier plans and window upgrade effectiveness.

2.28.2.3. The installation ATO needs to stay informed of facility projects, and should be included as a nonvoting member of the facilities working group.

2.29.2. (Added)(AETC) AT/FP factors will be primary considerations in the base comprehensive planning process, including traffic and entrance gate planning, area development planning, and facility siting.

2.31. DoD Standard 31 – Executive Protection and High Risk Personnel Security. The installation security council needs to evaluate the need to install duress systems, safe havens, and implementing code words to safeguard high-risk personnel. Identify high-risk personnel by position in the installation security plan.

Chapter 3 (Added)(AETC)

RECOGNITION PROGRAM AWARDS

3.1. (Added)(AETC) DoD AT/FP Recognition Program Awards. Each year, the Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (OASD SO/LIC) recognizes outstanding AT efforts and installation programs that clearly set precedence in the AT/FP field.

3.1.1. (Added)(AETC) Units wishing to submit nomination packages for these awards must forward them to HQ AETC/SFP no later than 20 February of the current calendar year.

3.1.2. (Added)(AETC) Nomination packages should include details covering the previous calendar year. HQ AETC/SFP will forward specific details and a notification message to AETC installations each year. Submissions should follow formatting instructions, and photographs with captions should be included to help accurately portray accomplishments.

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

AFI 10-2501, *Full Spectrum Threat Response (FSTR) Planning and Operations*

AFMAN 37-123, *Management of Records*

UFC 4-010-01, *DoD Minimum Antiterrorism Standards for Buildings*

UFC 4-010-10, *DoD Minimum Antiterrorism Standoff Distances for Buildings*

JOHANN R. KINSEY, Colonel, USAF
Director of Security Forces

6 Attachments (Added)(AETC)

9. HQ AETC Force Protection Working Group (FPWG)

10. HQ AETC Threat Working Group (TWG)

11. Installation AT/FP Program Continuity Book

12. Installation ATO/FP POC Checklist

13. Installation Standards for Barriers and Fencing

14. Mission, Symbolism, History, Accessibility, Recognizability, Population, and Proximity (MSHARPP) Matrix Explanation

Attachment 9 (Added)(AETC)**HQ AETC FORCE PROTECTION WORKING GROUP (FPWG)**

A9.1. (Added)(AETC) Purpose of the Force Protection Working Group (FPWG). This attachment covers operation of the HQ AETC FPWG. It applies to HQ AETC directors, chiefs of special staff, and members of the HQ AETC Crisis Action Team (CAT).

A9.1.1. (Added)(AETC) HQ AETC has established a FPWG to serve as the AETC commander's primary advisory body on AT policy and program management. The FPWG is a permanent, cross-functional group that is convened at least monthly. It may also be convened at the request of HQ AETC senior leadership or HQ AETC CAT director, and/or as local, national, and world events dictate.

A9.1.2. (Added)(AETC) Working group members are responsible for coordinating and providing deliberate planning for all command-level AT/FP issues. The FPWG reviews local, national, and worldwide threat information and intelligence, and prepares recommendations for the AETC commander (AETC/CC). These recommendations include, but are not limited to, increasing force protection (FP) conditions, implementing increased random antiterrorism (AT) measures (RAM), and other associated actions to protect the command's personnel, property, and information infrastructure from possible terrorist attacks.

A9.2. (Added)(AETC) Membership and Organization:

A9.2.1. (Added)(AETC) The FPWG functions as a subgroup of the HQ AETC CAT, and reports to the HQ AETC/SF. The FPWG operates independently until the HQ CAT activates. The HQ AETC/SF, or designated representative, chairs the FPWG, and keeps the HQ AETC CAT director informed of all FPWG activities. The FPWG chair coordinates AT and FP issues with the HQ AETC CAT, upon its activation.

A9.2.2. (Added)(AETC) The FPWG meets as required (but at least quarterly) to address AT and FP action items involving command forces worldwide. The group is comprised of representatives from each directorate and special staff within HQ AETC, and a designated representative of the HQ AETC CAT director. Directorate membership will include SF, SG, DP, CCP, CCX, EDA, 4th Region AFOSI, CE, SV, XP, DO, DOYI, LG, JA, SC, FM, PA, and special staff representatives from AFRS and AFSAT. All members are required to have a current appointment memorandum on file with the security forces directorate. Each FPWG member must possess, at a minimum, a Secret clearance, verified through his or her security manager.

A9.2.3. (Added)(AETC) HQ AETC/SFP is the executive secretary and OPR for the AETC AT and FP program. HQ AETC/SFP will produce minutes for each FPWG meeting (maintain minutes in accordance with AFMAN 37-123). When approved, distribute FPWG minutes electronically to FPWG members.

A9.3. (Added)(AETC) Objectives. The FPWG will provide a:

A9.3.1. (Added)(AETC) Single focal point in HQ AETC to furnish oversight and support for command AT/FP and information security programs.

A9.3.2. (Added)(AETC) Forum to discuss intelligence and other activities of international and domestic terrorist groups; militia, hate, and patriot groups; organized gangs, and any other threats to AETC assets.

A9.3.3. (Added)(AETC) Cross-functional approach for recommendations to the HQ AETC CAT and senior leadership on AT/FP issues.

A9.4. (Added)(AETC) Responsibilities:

A9.4.1. (Added)(AETC) The FPWG must be kept updated on AT, FP, and information operations (IO) issues affecting the command in order to provide timely recommendations to the command's senior

leadership. HQ AETC/SF, or designated representative, will brief the HQ AETC CAT director, HQ AETC/DS, AETC/CV, or AETC/CC, on FPWG recommendations.

A9.4.2. (Added)(AETC) The FPWG will use operational risk management when addressing threats and vulnerabilities, and making recommendations.

A9.4.3. (Added)(AETC) The FPWG chair will notify the HQ AETC CAT director of any recommended changes in FPCONs and IW conditions, or need to recall the HQ AETC CAT.

A9.4.4. (Added)(AETC) Each FPWG member will be appointed in writing, and have at least a Secret clearance verified through his or her security manager. Each appointment memorandum must identify primary and alternate members, security clearance, 24-hour contact numbers (home, cell, office), and e-mail addresses. Update FPWG rosters and provide a copy to the HQ AETC CAT director. FPWG members should be the individuals responsible for the AT program in their organization.

A9.4.5. (Added)(AETC) The FPWG members should share information with all personnel who have a valid clearance and a need to know. This should include functional counterparts at the installation level.

A9.4.6. (Added)(AETC) Each FPWG member should review the FPWG charter at least annually for accuracy and updating.

Attachment 10 (Added)(AETC)**HQ AETC THREAT WORKING GROUP (TWG)**

A10.1. (Added)(AETC) Purpose. HQ AETC has established a TWG to serve as the AETC commander's primary advisory body on antiterrorism threat issues. The TWG is a permanent, cross-functional group convened at least monthly, or as needed, to review current threat information, and recommend course of action to mitigate threats. It may also be convened at the request of HQ AETC senior leadership or HQ AETC CAT director, and/or as local, national, and world events dictate.

A10.1.1. (Added)(AETC) It applies to HQ AETC directors and chiefs of staff, and members of the HQ AETC Crisis Action Team (CAT).

A10.1.2. (Added)(AETC) The HQ AETC TWG reviews current local, national, and worldwide threat information and intelligence, and potential threats affecting AETC and USAF operations, personnel, and resources, then recommends course of action to the HQ AETC/SF directorate to mitigate and counter those threats. Recommendations and mitigations may include, but are not limited to, increasing FP conditions and implementing increased random antiterrorism measures (RAM), and other associated actions to protect the command's personnel, property, and information infrastructure from possible terrorist attacks. The HQ AETC TWG also provides threat information to the HQ AETC FPWG and other force protection-related working groups, as required.

A10.2. (Added)(AETC) Membership and Organization:

A10.2.1. (Added)(AETC) The TWG functions as a subgroup of the HQ AETC CAT and reports to the HQ AETC/SF directorate. The TWG operates independently. HQ AETC/SFP, or designated representative, chairs the TWG and keeps the HQ AETC/SF directorate informed of all TWG activities.

A10.2.2. (Added)(AETC) The following comprise the core membership of the TWG: HQ AETC SF, 4th Region AFOSI, CE, DOYI, and SC. HQ AETC/SG and staff representatives from AFRS and AFSAT may participate as determined by the TWG chairperson.

A10.2.3. (Added)(AETC) The HQ AETC IO TWG is part of the HQ AETC TWG and is the OPR for briefing and/or analyzing IO threats, and recommending countermeasures and information condition (INFOCON) changes to the AETC commander and the TWG. HQ AETC/SC is primarily responsible for collecting, assessing, and reporting on computer security (for example, viruses, attempted hacking, and overall state of the networks).

A10.2.4. (Added)(AETC) HQ AETC/SFP, is the executive secretary and OPR for the AETC TWG. This office will record minutes of each TWG meeting (maintain minutes in accordance with AFMAN 37-123). Once approved, distribute TWG minutes electronically to TWG members.

A10.3. (Added)(AETC) Objectives. The TWG will provide a:

A10.3.1. (Added)(AETC) Single focal point in HQ AETC to furnish threat and intelligence information for command AT/FP.

A10.3.2. (Added)(AETC) Forum to discuss intelligence, threat information, information conditions, and other activities of domestic and international terrorist groups; militia, hate, patriot groups, organized gangs, and any other threats to AETC personnel and assets.

A10.3.3. (Added)(AETC) Cross-functional approach for recommendations to the HQ AETC/SF directorate and senior AETC leadership on AT/FP issues.

A10.4. (Added)(AETC) Responsibilities:

A10.4.1. (Added)(AETC) The TWG must be kept updated on AT, FP, and IO issues affecting the command, in order to provide timely recommendations to the command's senior leadership. HQ AETC/SF, or designated representative, will brief the HQ AETC CAT director, HQ AETC/DS, AETC/CV or AETC/CC, on TWG recommendations as appropriate.

A10.4.2. (Added)(AETC) The TWG will use operational risk management assessment to address threats and vulnerabilities and make recommendations.

A10.4.3. (Added)(AETC) The TWG chair will notify the HQ AETC/SF directorate of any recommended changes in FPCONs and IW conditions.

A10.4.4. (Added)(AETC) Each TWG member will be appointed in writing and possess a Secret clearance, verified through his or her security manager. Each appointment memorandum must identify primary and alternate members, security clearance, 24-hour contact numbers (home, cell, office), and e-mail addresses. Update TWG rosters and provide a copy to the HQ AETC CAT director, as required. TWG members should be the individuals responsible for the AT program in their respective directorate or special staff.

A10.4.5. (Added)(AETC) The TWG membership should share information with all personnel who have a valid clearance and a need to know. This should include functional counterparts at the installation level.

A10.4.6. (Added)(AETC) The TWG members should review the TWG charter annually for accuracy and updating as necessary.

Attachment 11 (Added)(AETC)**INSTALLATION AT/FP PROGRAM CONTINUITY BOOK**

A11.1. (Added)(AETC) Responsibility. The installation antiterrorism officer (ATO) and unit/tenant organization AT officer/NCO are each responsible for maintaining an AT/FP program continuity book. This attachment provides a book template, and defines the contents and format for books maintained by the installation ATO and unit AT officer/NCO. Book contents are subject to review during MAJCOM staff assistance visits (SAV), IG inspections, and installation AT program reviews.

A11.2. (Added)(AETC) Continuity Book. The book will contain at a minimum, the following items:

A11.2.1. (Added)(AETC) Section 1. Memorandum of Appointment (update as changes occur). The installation ATO will also place letters of appointment for unit/tenant organization AT/officers and NCOs. Include a listing of all unit AT monitors in this section as well.

A11.2.2. (Added)(AETC) Section 2. Installation ATO, Unit AT Officer, and NCO Training. Retain copy of installation ATO Level II training certificate (installation ATO book), and record of Level I awareness training for unit, tenant organization, and AT officer/NCO (installation and unit books).

A11.2.3. (Added)(AETC) Section 3. Localized Wing FPCON Measures.

A11.2.4. (Added)(AETC) Section 4. Logs. Unit random antiterrorism measures (RAM) log (unit book), or results of monthly unit-level RAMs log review (installation ATO book). Unit AT officer/NCO will maintain a product (MS Excel spreadsheet is recommended) showing date, time, length and type of RAM conducted. The installation ATO will randomly monitor unit RAM logs to verify non-SF, as well as SF organizations are conducting RAMs. Maintain schedule for and results of RAM checks in this tab in the installation ATO binder. Recording RAMs in Section 4 does not relieve unit from requirement to call RAMs in to wing command post.

A11.2.5. (Added)(AETC) Section 5. Functional Review Reports. Unit AT officer/NCO and installation ATO will maintain results of AT program reviews conducted during MAJCOM SAVs and IG inspections.

A11.2.6. (Added)(AETC) Section 6. AT/FP Information, Memorandums, Messages. Pass-ons from base ATO (e-mails, memos), wing AT bulletin (if applicable), and installation ATO schedule for unit AT program reviews.

A11.2.7. (Added)(AETC) Section 7. AFIs. AFI 10-245/AETC Sup 1 and installation AT instruction.

A11.2.8. (Added)(AETC) Section 8. OIs. Locally developed unit operating instruction (if applicable).

A11.2.9. (Added)(AETC) Section 9. Installation ATO Annual AT Program Reviews. Units/installation ATO will maintain copies of most recent and previous calendar year's annual ATO reviews of unit AT programs (only reports specific to that unit will be maintained in unit binders).

A11.2.10. (Added)(AETC) Section 10. AT Exercise Reports. Maintain reports generated from unit and wing-level AT exercises in this tab.

A11.2.11. (Added)(AETC) Section 11. Meeting Minutes. All FPWG, TWG minutes, and other related minutes.

A11.2.12. (Added)(AETC) Section 12. Miscellaneous Items.

Attachment 12 (Added)(AETC)**INSTALLATION ATO AT/FP POC CHECKLIST**

A12.1. General. While not all inclusive, this checklist is designed to aid installation ATOs in managing their program. It represents a list of “smart questions” to ask unit AT representatives when reviewing their individual programs.

Unit AT/FP Representative Responsibilities	YES	NO	N/A
Force Protection POC			
Has the commander designated a unit AT/FP representative in writing?			
Has the appointment letter been forwarded to the installation ATO?			
Has the unit developed a folder or binder to maintain meeting minutes, AT plan and local AT OI?			
Is the unit participating in the Installation RAM Program?			
Does the unit have specific RAMS and checklists?			
AT/FP Level I Training Requirements and Reporting			
Have Level I AT training requirements been incorporated into unit ancillary training requirements?			
Is Level I training being documented?			
Are personnel in the unit scheduled for Level I training?			
AT/FP Deployment/TDY/Leave Requirements			
Has the unit deployment manager developed procedures to request a deployment briefing for personnel deploying?			
Are procedures outlined on the checklist being followed for all deployments and TDYs?			
Does the orderly room ensure AT/FP requirements are met prior to issuing TDY orders or leave authorization numbers?			
Is a method of communication established so increase in threat level can be relayed to personnel while on leave or TDY?			
Unit FPCON Procedures			
Has the unit developed procedures to implement increased force protection conditions and measures?			
Have shortfalls in manpower or materials need to meet FPCON requirements been identified?			
Are projects, purchases of equipment, and READY program requirements being worked to correct shortfalls?			
Has the unit developed bomb threat and emergency evacuation procedures for all facilities controlled by the unit?			
Do the procedures identify assembly areas at least 500' from the facility and			

Unit AT/FP Representative Responsibilities	YES	NO	N/A
post incident responsibilities?			
Are notification procedures in place to ensure all personnel are notified of changes to the FPCON?			

Attachment 13 (Added)(AETC)**INSTALLATION STANDARDS FOR BARRIERS AND FENCING****A13.1. (Added)(AETC) Barriers and Installation Gates:**

A13.1.1. (Added)(AETC) Installations not having permanent barriers at installation gates must develop a plan in concert with HQ AETC/CE to establish barrier configurations necessary to provide protection and allow for the flow of traffic. Installations not so equipped must identify their requirements via VAMP to HQ AETC/SFX for programming action.

A13.1.2. (Added)(AETC) 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.

A13.1.3. (Added)(AETC) Portable barriers should be used in conjunction with other tools, such as manually removable bollards. Manually removable bollards are recommended for gates because they can be easily installed and removed for storage near the gate's location, when available.

A13.1.4. (Added)(AETC) 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 bollards 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.

A13.1.5. (Added)(AETC) Bollards are also excellent barriers for temporarily closing roadways or parking lots. Manually removable bollards, if available, should secure unmanned installation gates. Jersey style concrete barriers should only be used if bollards are not available.

A13.2. (Added)(AETC) Installation Perimeter Fencing:

A13.2.1. (Added)(AETC) The standard for AETC installation perimeter fencing is Type A2 chain-link fencing as specified by AFH 32-1084, *Facility Requirements*. Anchor the fence 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.

A13.2.2. (Added)(AETC) Check the fence periodically to prevent vegetation from overgrowing, and erosion from causing gaps under the fence line.

A13.2.3. (Added)(AETC) Place installation warning signs along the fence line in accordance with AFI 31-101, *The Air Force Installation Security Program*. Keep signs in good repair, and post in local language where appropriate.

Attachment 14 (Added)(AETC)

MISSION, SYMBOLISM, HISTORY, ACCESSIBILITY, RECOGNIZABILITY, POPULATION AND PROXIMITY (MSHARPP) MATRIX EXPLANATION

A14.1. (Added)(AETC) MSHARPP Matrix. The purpose of the MSHARPP matrix is to analyze likely terrorist targets. Consideration is given to the local threat, likely means of attack available to the enemy, and variables affecting the disposition (for example, attractiveness to enemy, potential psychological effect on community, etc.) of potential targets. This document provides an example of how to use MSHARPP.

A14.2. (Added)(AETC) Selection Factors. After developing a list of potential targets, use the MSHARPP selection factors to assist in further refining your assessment by determining the most likely (for example, efficient, effective, and plausible) method of attack, and identifying vulnerabilities to that type of attack. After the MSHARPP values for each target or component are assigned, the sum of the values indicate the highest value target (for a particular mode of attack) within the limits of the enemy's known capabilities.

A14.3. (Added)(AETC) Mission. Mission focuses mainly on the threat to the situations, activities, capabilities, and resources on an installation to a terrorist attack. What is the importance of the area or assets, considering their function, inherent nature, and monetary value? What are the ramifications of a terrorist attack, considering the psychological, economic, sociological, and military impacts? How long will it take to recover from an attack, considering the availability of resources, parts, expertise and manpower, and redundancies? Assess points to the target equipment, information, facilities, and/or operations or activities (scale of 1-5; 5 being worst) in this area based upon the degree of mission degradation if attacked by a terrorist, (see Figure A14.1).

Figure A14.1. Mission Criteria.

CRITERIA	SCALE
Installation cannot continue to carry out its mission until the attacked asset is restored.	5
Ability to carry out a primary mission of the installation would be significantly impaired if this asset were successfully attacked.	4
Half of the mission capability remains if the asset were successfully attacked.	3
The installation could continue to carry out its mission if this asset were attacked, albeit with some degradation in effectiveness.	2
Destroying or disrupting this asset would have no effect on the ability of the installation to accomplish its mission.	1

A14.4. (Added)(AETC) Symbolism. Consider whether the target represents, or is perceived by the enemy to represent, a symbol of a targeted group (for example, symbolic of US military, Christianity, government, authority, etc.). Assess points in this area based upon the symbolic value of the target to the enemy (see Figure A14.2.).

Figure A14.2. Symbolism Criteria.

CRITERIA	SCALE
High profile, direct symbol of target group or ideology.	5
Low profile, direct symbol of target group or ideology.	3-4
Low profile and/or obscure symbol of target group or ideology.	1-2

A14.5. (Added)(AETC) History. Do terrorist groups have a history of attacking this type of target? While you must consider terrorist trends worldwide, focus on local targeting history and capabilities (see Figure A14.3).

Figure A14.3. History Criteria.

CRITERIA	SCALE
Strong history of attacking this type of target.	5
History of attacking this type of target, but none in the immediate past.	3-4
Little to no history of attacking this type of target.	1-2

A14.6. (Added)(AETC) Accessibility:

A14.6.1. (Added)(AETC) A target is accessible when an operational element can reach the target with sufficient personnel and equipment to accomplish its mission. A target can be accessible even if it requires the assistance of knowledgeable insiders (see Figure A14.4.).

A14.6.2. (Added)(AETC) This assessment entails identifying and studying critical paths the operational element must take to achieve its objectives, and measuring those things that aid or impede access. The enemy must not only be able to reach the target, but must also remain there for an extended period. The four basic stages to consider when assessing accessibility are:

A14.6.2.1. (Added)(AETC) Infiltration from the staging base to the target area.

A14.6.2.2. (Added)(AETC) Movement from the point of entry to the target or objective.

A14.6.2.3. (Added)(AETC) Movement to the target's critical element.

A14.6.2.4. (Added)(AETC) Exfiltration.

Figure A14.4. Accessibility Criteria.

CRITERIA	SCALE
Easily accessible, standoff weapons can be employed.	5
Inside perimeter fence, climbing or lowering required.	3-4
Not accessible or inaccessible without extreme difficulty.	1-2

A14.7. (Added)(AETC) Recognizability:

A14.7.1. (Added)(AETC) A target's recognizability is the degree to which it can be recognized by operational elements and/or intelligence collection, and reconnaissance assets under varying conditions. Weather has an obvious and significant impact on visibility (friendly and enemy). Rain, snow, and ground fog may obscure observation. Road segments with sparse vegetation and adjacent high ground provide excellent conditions for good observation. Distance, light, and season must be considered (See Figure A14.5).

A14.7.2. (Added)(AETC) Other factors influencing recognizability include the size and complexity of the target, the existence of distinctive target signatures, the presence of masking or camouflage, and the technical sophistication and training of the enemy.

Figure A14.5. Recognizability Criteria.

CRITERIA	SCALE
Target is clearly recognizable under all conditions and from a distance; requires little or no training for recognition.	5
Target is easily recognizable at small arms range and requires a small amount of training for recognition.	4
Target is difficult to recognize at night or in bad weather, or it might be confused with other targets; requires training for recognition	2-3
Target cannot be recognized under any conditions – except by experts.	1

A14.8. (Added)(AETC) Population. What is the population relative to other potential targets (see Figure A14.6)? Going on the assumption the intent of the attack is to kill or injure personnel, it follows that the more densely populated an area or facility is, the more lucrative a target it makes (all other things being equal).

Figure A14.6. Population Criteria.

CRITERIA	SCALE
Densely populated; prone to frequent crowds.	4-5
Relatively large numbers of people, but not in close proximity (for example, spread out and hard to reach in a single attack).	3
Sparsely populated; prone to having small groups or numbers of individuals.	1-2

A14.9. (Added)(AETC) Proximity. Is the potential target located near other personnel, facilities or resources that, because of their intrinsic value or protected status, and a fear of collateral damage, afford it some form of protection (for example, near national monuments, protected/religious symbols, etc., that the adversary holds in high regard) (see Figure A14.7)?

Figure A14.7. Proximity Criteria.

CRITERIA	SCALE
Target is in close proximity; serious injury/damage or death/total destruction of protected personnel/facilities likely.	5
Target is in close enough proximity to place protected personnel, facilities, etc., at risk of injury or damage, but not destruction.	3-4
Target is isolated; no chance of unwanted collateral damage to protected symbols or personnel.	1-2

NOTE: It is important to consider whether the target is in close proximity to other targets. Just as the risk of unwanted collateral damage may decrease the chances of attack, a target rich environment may increase the chances of unwanted attack.

A14.10. (Added)(AETC) Scoring. Add the scores across the rows to produce the MSHARPP score for that particular target to that mode of attack. Use this information to prioritize FP efforts, and in determining funding for FP projects.