

**BY ORDER OF THE COMMANDER
HILL AIR FORCE BASE (AFMC)**

AIR FORCE INSTRUCTION 31-210



**HILL AIR FORCE BASE
Supplement 1**

22 AUGUST 2000

Security

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

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the OO ALC WWW site at: <http://scsweb.hill.af.mil/pdl/pubs.htm>. Personnel with no access to electronic media may view the publication at the Base Master Publications Library, 75 CS/SCSP.

OPR: 75 SFS/SFOA (Mr. Paul Wagner)

Certified by: 75 SFS/SFOA
(Maj Warren L. Keithley, Jr.)

Pages: 8

Distribution: F

All agencies are required to participate in Hill's Antiterrorism/Force Protection Program (AT/FP), unless specifically exempted by the commander. The terms "must," "shall," and "will" denote mandatory actions in this supplement. Send comments and suggested improvements to 75th Security Forces Operations Flight (75 SFS/SFO), 6010 Gum Lane, Hill Air Force Base, Utah, 84056-5206 on *AF Form 847, Recommendation for Change of Publication*.

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

1.6. The Ogden Air Logistics Center Commander (OO-ALC/CC) retains overall responsibility for Hill Air Force Base's AT Program. However, authority is delegated to the 75th Air Base Wing Commander (75 ABW/CC) to implement an antiterrorism program at Hill AFB. This includes authority to implement and change appropriate threat conditions and measures.

1.8. Operations Security (OPSEC). Designated Critical Information (CI) relating to Antiterrorism/Force Protection shall be protected as stated below. Current CI list may be obtained from 75th Security Forces Operations Security (75 SFS/SFAI), your respective security manager, or facility security officer. CI protection requirements are:

1.8.1. (Added) PHONE. CI cannot be discussed over unsecured telephone lines, you must use a secure telephone.

1.8.2. (Added) FAX. CI can not be faxed over unencrypted fax machines.

1.8.3. (Added) RADIO. CI can not be discussed over unencrypted radio/cell phones.

1.8.4. (Added) EMAIL. CI can not be e-mailed in an unencrypted format, except in instances when the e-mail does not go "beyond the Hill firewall." In other words, you should not e-mail CI off base, even to

another government agency, unless you encrypt it by approved means. If your e-mail is on base, be sure to indicate to the recipients that the information contained in the e-mail is CI and/or For Official Use Only, and that they should keep that fact in mind if the e-mail is forwarded to other persons. CI must also be encrypted if sent over the Internet by any means.

1.8.5. (Added) STORAGE. When unattended, CI must be protected, in a locked office, desk, or cabinet.

1.8.6. (Added) DESTRUCTION. CI must be destroyed by shredding or burning.

3.1.1.4. (Added) The Hill Air Force Base Antiterrorism/Force Protection Working Group (AT/FP WG) serves as the commander's primary advisor on the terrorist threat. The AT/FP WG combines intelligence, counterintelligence, terrorism, and criminal and force protection agencies with execution personnel, into one comprehensive working group. The AT/FP WG is charged with assessing threat information and terrorist capabilities, as well as, the overall effectiveness of the installation's AT/FP program.

3.1.1.4.1. (Added) The AT/FP WG is formally chartered and will consist of members representing the Air Force Office of Special Investigation (AFOSI), 75th Security Forces (75 SFS), 75th Civil Engineering Group (75 CEG), Ogden Air Logistics Center Technical and Industrial Operational Flight (OO-ALC/TISFB), Ogden Air Logistics Center Staff Judge Advocate (OO-ALC/JA), Ogden Air Logistics Center Public Affairs Office (OO-ALC/PA), Ogden Air Logistics Center Inspector General (OO-ALC/IG), Ogden Air Logistics Center Plans (OO-ALC/XP), 75th Transportation Division, (75 TRANS/LGT), Ogden Air Logistics Center Financial Management and Comptroller Directorate (OO-ALC/FM), 75th Medical Group (75 MDG/SG), and 75th Communications Squadron (75 CS). Additional functional representatives may participate in AT/FP WG proceedings on an as required basis. Within the AT/FP WG, 75 SF, TISFB, 75 CS, and AFOSI will make up the threat working group (TWG) and are responsible for assessing threat information. The chief of security forces or AT/FP Officer will chair the AT/FP WG.

3.1.1.4.2. (Added) The site director at survivability and vulnerability integration center (SVIC) and the Utah Test and Training Range (UTTR) should obtain threat assessment information applicable to the local area from law enforcement agencies and the AFOSI Detachment at Hill AFB, UT. The SVIC and UTTR site director will inform 75 SFS/SFO of any changes in the current local threat assessment.

3.2.4. The force protection working group will submit an AT/FP budget through the installation commander.

3.3.4.1. The OO-ALC Exercise Evaluation Team (EET) Team Chief, in conjunction with the AT focal point, will exercise AT/FP plans to test a broad range of THREATCON and INFORMATION COMMUNICATIONS (INFOCON) procedures contained within applicable plans at least semi-annually. The EET Chief will provide feedback as appropriate concerning the overall effectiveness of the installation's AT/FP program, to include dissemination of threat information. SVIC and UTTR will participate in exercises conducted by the 75 ABW or other agencies, as determined by the site director.

3.3.4.2. OO-ALC/PA personnel will disseminate information to the public at the first indication of a terrorist incident or upon commander's direction. OO-ALC/PA should consider procedures listed in paragraphs 1.8 to 1.8.6 of this supplement in order to control information, measures, procedures and observable actions about friendly forces capabilities, limitations and intentions.

3.4.5. Organizations should review all host/tenant agreements for local emergency support to ensure anti-terrorism procedures are covered. A copy will be forward to the 75 SFS/SFO, Hill AFB AT/FP representative for review and file.

3.5.2. 75 SFS is the primary OPR for publishing, reviewing, and updating the Hill AFB Installation Security Plan (ISP) and Instruction (ISI). All *Hill AFB Plans* will include or cross reference disaster response force procedures contained in *Hill AFB OPLAN 32-1, Emergency Management*. *Hill AFB OPLAN 32-1* will also contain contingency plans for responding to incidents involving weapons of mass destruction (WMD). All plans will be reviewed annually, NLT 31 December of each year. Copies of all *Hill AFB Plans* dealing with AT/FP will be coordinated and a final copy provided to 75 SFS/SFO, when developed or revised.

3.6.3.1. The AT/FP WG will direct subordinates to plan and program corrective action as appropriate. Any AT/FP vulnerabilities having a low-cost fix must be programmed and budgeted to improve AT/FP posture. This action will be reviewed NLT 31 Aug annually and reported to the AT/FP Office via e-mail.

3.8.2. All personnel with information or knowledge of information, individuals, events, or situations that could pose a threat to the security of Hill AFB personnel and/or resources will report this information to AFOSI at extension 777-1852 or Security Forces at ext. 777-3056 immediately. Survivability and vulnerability integration center (SVIC) and UTTR personnel shall report this information to the site director or other designated personnel.

3.8.2.2. The installation commander has tasked DET 113, AFOSI to collect, analyze, and disseminate terrorist threat information to include potential terrorist use of WMD.

3.12.3. The Hill AFB TWG may use the guide (Attachment 7) to this supplement when assessing terrorist threat information.

3.13.1. The TWG uses locally developed information and the analysis provided by the various agencies within the intelligence community, including the Federal Bureau of Investigation (FBI) and local law enforcement agencies, to arrive at a local threat assessment. Compiling and examining all available information will be a continual and ongoing process.

3.13.1.5. All OO-ALC special events will be subjected to force protection scrutiny by the AT/FP Installation Officer (75 SFS/SFO). Organizers will include the designated focal point when planning such activities for recommendation and inclusion of appropriate AT/FP measures.

3.14.2. The chief of security forces (75 SFS/CC) is the primary focal point for preparing and updating the Hill AFB, SVIC, and UTTR vulnerability assessments as required. The assessment team will include representatives from 75 SFS, AFOSI, 75 CEG, OO-ALC/TISFB, 75 MDG, and 75 CS, as a minimum.

3.20.1. Hill AFB 75 CEG will ensure all new construction projects and existing building rehabilitation employ AT/FP features where and when possible. This includes facilities at SVIC and UTTR.

3.20.2.1.1. (Added) 75 SFS/SF will conduct a review of all new construction and major rehabilitation projects for compliance with AT/FP construction standards and any additional force protection requirements. The FPWG will approve/disapprove any recommendations, based on a cost and risk analysis for force protection enhancements. Where an agreement cannot be reached between the AT focal point and respective agencies/program managers, 75 SFS/SF will submit comments for review by the FPWG to the 75 ABW/CC.

3.23.4. The 75 SFS/CC will chair the Hill AT/FP WG.

3.24.7. 75th Mission Support, Personnel Readiness Function (75 MSS/DPMAR-O) will ensure AT Level I training is accomplished prior to final out-processing for all military personnel departing to an overseas location. AFOSI, DET 113 is responsible for conducting Level I AT training.

3.24.8. All units will develop a procedure, ensuring all personnel are trained on area of responsibility (AOR) specific terrorist and medical threats prior to departing home stations for TDY, permanent change of station (PCS), or traveling outside the CONUS.

3.24.8.1. AT/FP required training will be accomplished and documented as stated below:

3.24.8.1.1. AT LEVEL I TRAINING FOR GOVERNMENT EMPLOYEES. AT/FP Level I training is required for all Hill AFB government employees and their family members (when family members are deploying or traveling on government orders) within six months of any deployment, leave, or travel outside the continental United States (includes Alaska, Hawaii, and US territories). Employees requiring Level I training should contact AFOSI at extension 777-1852 to schedule the training. Individuals should schedule this training as soon as they become aware that they will be traveling overseas. Generally, a 30-day notice is requested. After receiving Level I training, employees must provide proof of completion to 75 MSS/DPMAR-O for entry into PC III. Sponsors are responsible for ensuring their family members receive all mandatory training prior to official travel or leave overseas. The unit security manager (USM) will maintain a roster of all personnel completing the training.

3.24.8.1.2. (Added) AT/LEVEL I TRAINING FOR SVIC/UTTR PERSONNEL. At Level I training, as required above in paragraph 3.24.8.1.1 will be conducted by the AFOSI Detachment at Hill AFB, UT. The USM will maintain a roster of all personnel completing the training.

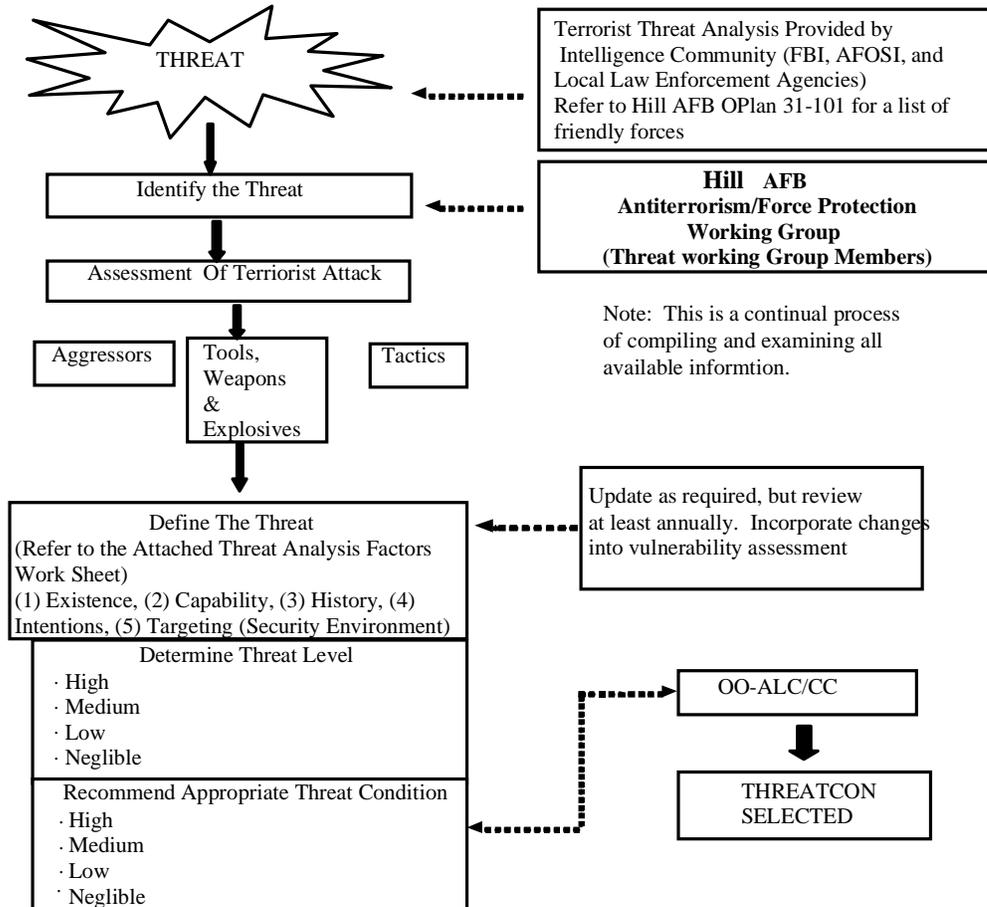
3.24.8.4. GENERAL AT/FP AWARENESS. General AT/FP awareness training is mandatory for all OO-ALC government personnel. The USM will conduct this training annually using approved training material supplied by 75 SFS/SFO. Documentation of completion of general awareness training is also mandatory and will be maintained by the respective USM. Certification of completed training will be sent to 75 SFS/SFO by 31 December of each year.

3.25.3. All commanders and two digit directors responsible for government and contractor personnel, will implement procedures to prohibit publication of orders for overseas travel for those personnel who have not received the required training.

3.26.4. As a minimum, the itineraries of all visiting general officers and DAF civilian equivalents will be marked "For Official Use Only." Access to specific details concerning travel arrangements will be restricted to those personnel with a "need-to-know." Consult with 75 SFS/SFO if additional guidance is required when preparing travel itineraries for high-risk personnel to high-threat areas.

Attachment 1 - Terms. Critical Information -- Critical information is information about friendly (U.S., allied, and/or coalition) activities, intentions, or limitations that an adversary needs in order to gain a military, political, diplomatic, or technological advantage. Such information, if released to an adversary prematurely, may prevent or forestall mission accomplishment, reduce mission effectiveness or cause loss of lives and/or damage to friendly resources. CI usually involves a few key items of friendly activities or intentions that might significantly degrade mission effectiveness. CI may also be derived from bits and pieces of related information (indicators).

**Attachment 7 (ADDED)
THREAT ASSESSMENT AND THREATCON SELECTION PROCESS**



THREAT LEVEL DEVELOPMENT

Level	Existence	Capability	Intentions	History	Targeting*	Security Environ.
Negligible	May be present	May be present				
Low	Must be present	Must be present		May be present		
Medium	Must be present	Must be present	May be present	Must be present		
High	Must be present	Must be present	Must be present	Must be present	May be present	
Critical**	Must be present	Must be present	Must be present	May be present	Must be present	

*Specific target information is not generally available

**This threat level is the only level where specific targeting information is present. Installation commanders must take appropriate protective measures at this level.

- **Existence.** A terrorist group is present, assessed to be present, or able to gain access to a given country or locale.
- **Capability.** The acquired, assessed, or demonstrated level of capability for a terrorist group to conduct attacks.
- **Intentions.** Demonstrated anti-US terrorist activity or states an assessed desire to conduct such activity.
- **History.** Demonstrated terrorist activity over time.
- **Targeting.** Current, credible information on activities indicative of preparations for specific terrorist operations.
- **Security Environment.** The internal, political and security considerations that impact on the capability of terrorist elements to carry out their intentions.

FILL IN THE EXSISTING FACTORS:

Threat Analysis Factors					
THREAT LEVEL	Existence	Capability	History	Intentions	Targeting
CRITICAL					
HIGH					
MEDIUM					
LOW					
NEGLIGIBLE					
Assessment of the Current Threat Level: _____					

Note 1: The installation must assess the terrorist threat by querying its intelligence system, local law enforcement, and federal agencies to determine its threat level. The above table provides some basic guidelines for determining the Threat Level based on the six analysis factors. Specific threat level information and guidance can be found in DoD 0-2000.12-H, Chapter 5.

Note 2: During the assessment, it may also be useful to try and link identified threats to a *specific time period or location*. For example, a terrorist group operating in the proximity of the installation may typically target areas which contain a large number of personnel, such as the club or the commissary. With this knowledge, the TWG should pay close attention to vulnerabilities in these areas.

KENNETH M. PAGE, Colonel, USAF
Commander, 75th Air Base Wing