

**BY ORDER OF THE  
SECRETARY OF THE AIR FORCE**

**AIR FORCE INSTRUCTION 31-210**

**1 AUGUST 1999**



**AIR FORCE RESERVE COMMAND  
Supplement 1**

**15 July 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 HQ AFRC WWW at: <https://wwwmil.afrc.af.mil> and the AFRCEPL (CD-ROM) published monthly.

---

OPR: HQ USAF/XOFP (Col Salley)  
Supersedes AFI 31-210, 1 July 1997

Certified by: HQ USAF/XOF (Brig Gen Coleman)  
Pages: 53  
Distribution: F

---

This instruction implements AFPD 31-2, *Law Enforcement*; DoDD 2000.12, *DoD Antiterrorism/Force Protection (AT/FP) Program*, April 13, 1999; DoDI 2000.14, *DoD Combating Terrorism Program Procedures*, June 15, 1994; DoDI 2000.16, *DoD Combating Terrorism Program Standards*; and DoD 0-2000.12-H, *Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence*, February 1993. It establishes responsibilities and guidance for the Air Force AT/FP Program and integrates security precautions and defensive measures. This Air Force Instruction applies to Air Force Reserve Command (AFRC) and Air National Guard units.

---

(**AFRC**) The OPR for this supplement is HQ AFRC/SFOF (Maj Mark S. Gunzelman). This supplement implements and extends guidance of Air Force Instruction (AFI) 31-210, 1 August 1999. The AFI is published word for word without editorial review. Air Force Reserve Command supplementary material is indicated by "(AFRC)" in boldface type. This supplement describes Air Force Reserve Command procedures to be used in conjunction with the basic instruction. Upon receipt of this supplement discard the Air Force basic

**SUMMARY OF REVISIONS**

**This document is substantially revised and must be completely reviewed.**

It incorporates the antiterrorism/force protection standards of DoDI 2000.16 and provides additional Air Force specific guidance on their implementation.

1. Air Force AT/FP (AT/FP) Program .....	2
2. DoD Policy .....	3

3. DoD and Air Force Established Standards ..... 3

Table 1. PRE-DEPLOYMENT & CAREER DEVELOPMENT AT/FP TRAINING REQUIREMENTS ..... 24

**Attachment 1— GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 33**

**Attachment 2— REFERENCES TO DOD O-2000.12-H 40**

**Attachment 3— TERRORISM THREAT CONDITIONS (THREATCONS) 42**

**Attachment 4— TERRORIST THREAT ASSESSMENT GUIDELINES 46**

**Attachment 5— AOR-SPECIFIC TRAINING 48**

**Attachment 6 (Added-AFRC)— DEMOGRAPHY, SYMBOLISM, HISTORY, ACCESSIBILITY, RECOGNIZABILITY, POPULATION, AND PROXIMITY (DSHARPP) MATRIX EXPLANATION 50**

**1. Air Force AT/FP (AT/FP) Program.** The program seeks to deter or blunt terrorist acts against the US Air Force by giving guidance on collecting and disseminating timely threat information, providing training to all AF members, developing comprehensive plans to deter, counter and recover from terrorist incidents, allocating funds and personnel, and implementing defensive measures.

1.1. The US position on terrorism is to deter terrorism in all its forms, wherever it takes place. National security decision directives as well as the statements by the President and senior officials set forth this policy. This instruction implements DoDI 2000.16, *The DoD Combating Terrorism Program Standards*, with added Air Force-specific standards.

1.2. The US Government is opposed to domestic and international terrorism and is prepared to act in concert with other nations or unilaterally when necessary to prevent or respond to terrorist acts.

1.3. The US Government considers the practice of terrorism by any person or group presents a potential threat to US national security. It will resist the use of terrorism by all legal means available. If there is evidence that a state is mounting or intends to conduct an act of terrorism against this country, the United States will take measures to protect its citizens, property, and interests.

1.4. The US Government is to make no concessions to terrorists. At the same time, the United States will use every available resource to gain the safe return of American citizens held hostage by terrorists.

1.5. The United States will act in a decisive manner against terrorists without surrendering basic freedoms or endangering democratic principles, and will encourage other governments to take similar stands.

1.6. Antiterrorism/force protection is a command responsibility and must be thoroughly integrated into every unit's mission. Commanders must continually review their antiterrorism/force protection posture with current and changing policy and threat levels. Risk management, based on the threat, is key in determining vulnerability and prioritization of resources. Any hazard with a level of risk that cannot be controlled to an acceptable level must be forwarded to the next level in the chain of command for resolution. Antiterrorism/Force Protection also requires every individual to maintain a level of awareness, to practice personal security measures, and to report suspicious activity.

**1.6. (AFRC)** AFRC installation commanders are responsible for the AT/FP program at their respective installation.

1.7. Countering the terrorist threat requires a fully integrated and coordinated force protection approach with a number of key functional areas including, at a minimum: Civil Engineering, Communications, Intelligence, Operations, Security Forces, Surgeon General, Judge Advocate, and the Air Force Office of Special Investigations.

**1.8. (Added-AFRC)** Operations Security (OPSEC). The goal of OPSEC is to control information and observable actions about friendly force capabilities, limitations, and intentions so as to prevent or control their exploitation by an adversary. OPSEC must be incorporated throughout the entire AT/FP program. Air Force OPSEC policy is located in AFI 10-1101, *Operations Security*.

**1.9. (Added-AFRC)** Force Protection Performance Measures (FPPM). The Air Staff Security Forces/Force Protection Division (HQ USAF/XOFP) develops, implements, tracks, and reports the status of the Air Force's Force Protection Program (AF FPP). The purpose of the FPPMs is to mark milestones in the program and, as markers are met, FP measures will be discontinued and new ones established as needed. HQ USAF/XOFP identifies measures to be reported by message to the MAJCOM semi-annually during October and April. HQ AFRC/SF provides the FPPMs to the installation AT/FP Officer prior to the data call. The installation AT/FP officer collects and compiles the information required by the FPPM and provides it to HQ AFRC/SF by the 15th day of the reporting month.

**2. DoD Policy .** DoDD 2000.12, *DoD Antiterrorism/Force Protection (AT/FP) Program*, establishes the DoD policies and responsibilities for the implementation of the DoD combating terrorism program. It establishes DoDI 2000.16, *Combating Terrorism Program Standards*, and DoD 2000.12-H, *Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence*.

**3. DoD and Air Force Established Standards.** The following antiterrorism/force protection standards incorporate the DoD standards from 2000.16 and provide further Air Force specific guidance on their implementation. Air Force implementation of the DoD standards is contained in the following starred subparagraphs.

3.1. DoD Standard 1 – DoD Antiterrorism and Force Protection Policy (AT/FP). Combatant Commanders, Chiefs of Service, and Directors of DoD Agencies and Field Activities (CINC/Service/Agency) are responsible for the implementation of DoD Antiterrorism/Force Protection (AT/FP) policies within their organizations.

3.1.1. AF Deputy Chief of Staff, Air & Space Operations (AF/XO), is the OPR for antiterrorism/force protection matters and policy.

3.1.1.1. The Air Staff, through the Air Staff Force Protection Working Group (FPWG), will serve as the primary organization to discuss and coordinate force protection matters designed

to organize, equip and train the force. The Working Group is the primary body to advise the CSAF on AT/FP matters. The Working Group will be chaired by a general officer steering group of AF/XOF and AF/XOP. As a minimum, the Working Group will consist of representatives from the following force protection core functional areas: IGX, ILE, SGX, SCX, JAI, XOF, XOI, and XOO. In addition, representatives from DPD, FMB, ILT, XOJ, XON, XOR, and XPM, will participate in meetings that affect their functional expertise.

**3.1.1.2. (Added-AFRC)** At HQ AFRC, the Force Protection Board (FPB) serves as the primary body to advise the AFRC/CC/CV on AT/FP matters. The Director of Security Forces (AFRC/SF) chairs the FPB. As a minimum, the board consists of representatives from the following core functional areas: CE, DO, DOI, DOZ, FM, LG, SC, SG, SF, AFOSI, and XP. In addition, associate members are requested to attend from the following functional areas: DP, HC, HO, IG, JA, PA, SE, SV, and RS.

3.1.2. The Director of Security Forces (AF/XOF):

3.1.2.1. Drafts and coordinates policy with the Air Staff FPWG and appropriate functional experts. AF/XO will approve all Air Force-wide AT/FP programs.

3.1.2.2. Develops guidance on antiterrorism/force protection and physical security enhancements.

3.1.2.3. Monitors program element (PE) 28047 and coordinates funding for AT/FP initiatives with Air Staff functional experts for XO approval.

3.1.2.4. Evaluates antiterrorism equipment and supplies in conjunction with other FP functional areas.

3.1.3. Air Force Surgeon General (AF/SG). Sets medical support requirements for antiterrorism planning and for personal force health protection.

3.1.4. Air Force Director of Transportation (AF/ILT). Coordinates policies affecting DoD Travel Security Policy and issues changes to all MAJCOMs and FOAs. Distributes DoD Travel Advisories (TSA), and retransmits Office of the Assistant Secretary of Defense Special Operations/Low Intensity Conflict (OASD(SO/LIC)) messages regarding travel advisories. AF/ILT helps staff and coordinate authorizations for non-tactical armored vehicles.

3.1.5. Air Force, Deputy Chief of Staff, Air and Space Operations (AF/XO):

3.1.5.1. Air Force Director of Intelligence, Surveillance, and Reconnaissance (AF/XOI). Establishes policies and guidelines for gathering and disseminating current foreign intelligence on international terrorism.

3.1.5.2. Air Force, Deputy Chief of Staff, Air & Space Operations, Director of Expeditionary Air Force Implementation (AF/XOP):

3.1.5.2.1. Monitors worldwide terrorism incidents.

3.1.5.2.2. Addresses security and counterterrorism issues in operations plans and publications, where appropriate.

3.1.5.2.3. Relays to senior USAF leadership, short and long-term measures to combat terrorism recommended by AF/XOF and AFOSI.

3.1.6. Secretary of the Air Force Public Affairs (SAF/PA) engages public affairs personnel to inform the public at the first indication of a terrorist incident.

3.1.7. Air Force Office of the Judge Advocate General (AF/JA) provides legal advice on AT/FP through the International and Operations Law Division (AF/JAI).

3.1.8. Headquarters, AFOSI, provides antiterrorism training; counterintelligence and terrorism investigations; threat information collection, analysis, and assessment; and specialized protective services; and local threat assessments and briefings. HQ AFOSI also serves as the focal point for the USAF Non-Tactical Armored Vehicle Program.

3.1.9. Air Force Director of Supply (AF/ILS). Assists HQ AFOSI in programming for supply and equipment requirements necessary for implementation of Air Force AT/FP policy requirements and assists HQ AFOSI in programming for non-tactical armored vehicles.

3.1.10. Air Force Civil Engineer (AF/ILE) is the OPR for nuclear, biological, and chemical defense matters and policy. Provides civil engineering expertise in the development of AT/FP policy issues. Provides AT/FP guidance to MAJCOMs for all new and existing construction standards that incorporate AT/FP measures ensuring the safety of personnel and resources. Provides AT/FP guidance to MAJCOMs for expedient AT/FP methods to use during contingency operations. Provides a core member to the Air Staff FPWG to provide civil engineering expertise as required.

3.1.11. Commanders at all echelons will develop a full working knowledge of AT/FP policies and standards.

**3.1.11.1. (ADDED-AFRC)** Wing/Installation commanders are responsible for the implementation of AT/FP policies within their organizations. AFRC NAF/CCs will ensure AT/FP policies are established and adhered to relative to contingency and readiness operations.

3.2. DoD Standard 2 – Development of CINC/Service/Agency Standards. CINC/Service/Agencies shall use standards contained herein as a baseline to develop specific standards with CINC/Service/Agency-unique requirements to fully implement their AT/FP program.

3.2.1. As a minimum, these standards should address the following areas:

3.2.1.1. AT/FP plans, Threat Assessment plans, and Incident Response plans.

3.2.1.2. Procedures to identify physical security requirements and to program for resources necessary to meet security requirements.

3.2.1.3. New construction.

3.2.2. AF/XOFP is OPR for the AFI which implements the 33 DoD prescriptive standards.

3.2.3. All commanders, down to installation commanders will publish a supplement to this instruction implementing further prescriptive standards in AT/FP for command and installation-unique requirements to fully incorporate these standards into their programs. These standards will include plans/annexes to implement the DoD and Air Force AT/FP initiatives, threat assessment procedures, and response measures to terrorist incidents. As a minimum, in addition to the requirements of Standard 2, plans will include: security and law enforcement assets, fortifications, sensors, obstacles, contract/hired forces, unit guards and on-call support from reaction forces, AT/

FP training and education, vulnerabilities and associated countermeasures (classified annex), installation priorities, host nation and local coordination. Plans will be reviewed annually.

**3.2.3. (AFRC)** AFRC Installation commanders must also develop a barrier plan for the protection of key facilities on their installation. The plan must address the specific location and placement of barriers, where they will be stored, and who is responsible to put them in place. This plan will be an annex to the Installation Security Plan (ISP) or the Installation AT/FP plan and should outline implementation procedures from THREATCON NORMAL through DELTA.

3.2.4. The Deputy Assistant Secretary of the Air Force (Budget) (SAF/FMB) includes approved antiterrorism budget requests in budget submissions, tracks program execution, and provides policy and guidance on legal limitations, and obligation criteria.

**3.2.4. (AFRC)** Installation commanders must budget for force protection requirements locally. If installations cannot fund force protection initiatives locally they forward them to HQ AFRC through their NAF as an unfunded requirement.

3.2.4.1. The Combating Terrorism Readiness Initiatives Fund (CbTRIF) provides a means for CINCs to react to unanticipated requirements due to changes in terrorist threat level or force protection doctrine/standards. It is not intended to subsidize ongoing projects, supplement budget shortfalls, or to support routine activity that is normally a Service responsibility. Funds may be requested by a combatant command (CINC) for requirements arising in the CINC's geographic or functional area of responsibility (AOR). Every Air Force command that serves as a component to a combatant command must coordinate requests in compliance with the CbTRIF program guidelines. At the same time a MAJCOM submits a request to the CINC, the MAJCOM shall also provide a copy to SAF/FMBO and AF/XOFP. Once a submission is initially processed by the Joint Staff (J-34), it shall be sent to the appropriate offices (Air Staff functionals) for coordination. SAF/FMBO will coordinate on requests and annotate whether or not Air Force funds are available. Detailed procedures and fund submission formatting instructions can be found in CJCS Instruction 5261.01A, Combating Terrorism Readiness Initiatives Fund.

3.3. DoD Standard 3 – Assignment of AT/FP Operational Responsibility. CINC/Service/Agencies shall clearly establish operational responsibility for AT/FP for all units and individuals whether permanently or temporarily assigned. When the responsibilities for force protection of the CINC/Service/Agencies overlap and are not otherwise governed by law or specific DoD policy, the affected parties may resolve the conflict by executing an appropriate memorandum of agreement.

3.3.1. Major Commands and Field Operating Agencies (MAJCOM and FOA) will identify in their supplement to this instruction specific operational responsibility for AT/FP down through the installation level for all persons permanently and temporarily assigned. MAJCOMs/FOAs will determine the scope of the force protection programs for facilities, operations, etc., which do not meet the legal definition of an installation.

**3.3.1. (AFRC)** Within AFRC, AT/FP operational responsibility rests with the AFRC/CC/CV, NAF/CCs (during wartime planning), and down to installation and squadron commanders. Where AFRC facilities don't meet the criteria of an installation, the senior ranking person (military or civilian) has AT/FP operational responsibility.

3.3.2. MAJCOMs and FOAs will ensure actions to combat terrorism outside the United States or in conjunction with other CINCs/Services/Agencies comply with applicable status of forces agreements (SOFA), the DoD Foreign Clearance Guide, and memoranda of understanding.

3.3.3. MAJCOMs and FOAs will work with other Air Force organizations, US service branches, and Department of Defense (DoD) agencies to reduce vulnerability to terrorism. MAJCOMs and FOAs must establish an antiterrorism program tailored to the local mission, conditions, the terrorist threat, and the national security environment.

3.3.4. Installation Commanders will:

3.3.4.1. Implement an AT/FP program to combat the local terrorist threat and support the US Air Force AT/FP program. This program should identify tasked agencies, required actions, and a means of exercising and evaluating the program through annual operational and command post antiterrorism exercises.

**3.3.4.1. (AFRC)** Conduct AFRC installation-wide antiterrorism exercises (both operational and command post) semiannually, as a minimum. Conducting and evaluating these exercises together may fulfill this requirement. Use exercises to test and evaluate the installation's ability to respond to the local terrorist threat. Exercises will test a broad range of required THREATCON actions specified within the installation's local plans and may be combined with other base exercises such as a MARE, BROKEN ARROW, etc. As a minimum, conduct one of these exercises during a unit training assembly (UTA).

3.3.4.2. Establish an active public affairs program to combat terrorism. Public affairs people are the primary spokespersons for the installation commander. Public Affairs should help dispel rumors and misinformation by providing appropriate and timely information to the news media and the base populace, according to current Office of Assistant Secretary of Defense for Public Affairs and SAF/PA antiterrorism guidance. Public Affairs Officers must stay current on the subject of terrorism to enhance their effectiveness in dealing with this issue.

3.3.4.3. Provide assistance when directed or requested by the lead agency. The lead agency for terrorist incidents outside the United States is the Department of State. The Department of Justice is the lead agency for incidents within the United States. The Federal Aviation Administration is the lead agency for certain aviation incidents.

3.4. DoD Standard 4 – AT/FP Coordination in Overseas Locations. CINC/Service/Agencies in overseas locations shall coordinate their AT/FP efforts with host nation authorities and the U.S. Country Team as appropriate. DoD intelligence and counterintelligence elements will coordinate their activities in support of AT/FP plans and programs through established DoD procedures in DoDI 5210.84.

3.4.1. CINCs, with geographic responsibilities, shall coordinate force protection matters with Chiefs of Mission (COMs), for countries within their area of operations, and with functional CINCs and Defense Agencies whose forces are stationed in or transit the CINC's AOR.

3.4.2. In those countries in which the Chief of Mission (COM) has force protection responsibilities for DoD elements the State Department's Overseas Security Policy Board (OSPB) security standards shall apply per Reference DoDI 5210.84.

3.4.3. The Director of the Defense Intelligence Agency acting as DoD's executive agent for diplomatic security matters, through the United States Defense Representative (USDR), shall ensure

that non-CINC assigned DoD elements, whose force protection responsibility rests with the COM, comply with OSPB standards per Reference DoDI 5210.84.

3.4.4. In those countries covered by the Memorandum of Understanding between the Department of State (DoS) and the Department of Defense on Security on the Arabian Peninsula dated 15 September 1996 (Reference MOU between DoD and DoS, 15 Sep 96), or any subsequent written agreement between DoS and DoD based on this MOU, the designated DoD representative for resolution of disputes with DoS officials is the Deputy Assistant Secretary of Defense for Policy and Missions (DASD (P&M)). CINCs who have concerns about Department of State standards shall bring them to the attention of the DASD (P&M) through the Joint Staff.

3.4.5. MAJCOMs and FOAs will ensure all agreements for local and host nation support are in writing and signed by appropriate civilian and military officials for CONUS and OCONUS installations.

3.5. DoD Standard 5 – Comprehensive AT/FP Program Development and Implementation. CINC/Service/Agencies shall develop and implement a comprehensive AT/FP program for personnel under their respective control designed to accomplish all the standards contained in this document. The program shall include a series of well-defined plans that describe and implement the program.

3.5.1. This instruction does not specify the format for AT/FP plans. However, plans will clearly describe force protection measures. These plans will be written from the CINC level down to the installation level for permanent operations or locations, and in operations orders (OPORDS) for temporary operations or exercises. At a minimum, these plans will include:

3.5.1.1. Procedures to collect and analyze terrorist threat information, threat, capabilities, and vulnerabilities to terrorist attacks;

3.5.1.2. Procedures for enhanced AT/FP protection; and

**3.5.1.2. (AFRC)** AFRC Installation commanders ensure a plan is developed for the protection of personnel and key facilities during increased THREATCONS.

3.5.1.3. Integrated procedures for security, fire, medical, command and control, and other emergency services to respond to terrorism incidents.

3.5.2. All commanders, down to installation commanders, will develop and implement AT/FP plans and or annexes to existing plans as outlined in these standards. Guidelines on AT/FP planning are found in AFMAN 10-401, Volumes 1 & 2.

3.6. DoD Standard 6 –Higher Headquarters Vulnerability Assessment of Installations and Review of Subordinate AT/FP Programs.

**3.6. (AFRC)** HQ AFRC will establish a vulnerability assessment team (VAT) to conduct assessments of AFRC installations.

3.6.1. Assessment Focus. The focus of the assessment will be the assessed unit's overarching AT/FP program. Assessments conducted to meet the requirements of this standard complement but do not replace the local comprehensive installation physical security vulnerability assessment required by Standard 14 of this instruction. AT/FP programs shall be subject to continual evaluation to avoid complacency and gain benefit from experiences from other assessments. Evolving terrorism threats, changes in security technology, development and implementation of alternative concepts of peacetime operations, and changing local conditions make periodic review essential.

CINC/Service/Agencies shall review lower level AT/FP Programs at least once every three years to ensure unity of AT/FP efforts throughout their AORs or subordinate commands.

3.6.1.1. AT/FP Assessment Areas. AT/FP vulnerability assessments provide a threat-based analysis of an activity's AT/FP program. The assessment identifies, for the commander, vulnerabilities that may be exploited by terrorists and suggests options that may eliminate or mitigate those vulnerabilities. Vulnerability assessments conducted to meet the requirement contained in this standard must assess as a minimum the following functional areas:

3.6.1.1.1. Counterintelligence, Law Enforcement Liaison, and Intelligence Support. The assessment will focus on the activity's ability to receive threat information and warnings from higher headquarters and local resources, actively collect information on the threat (when permitted and in accordance with applicable law and regulations), process that information to include local fusion and analysis, and develop a reasonably postulated threat statement of the activity. Further, the assessment will examine the ability to disseminate threat information to subordinate commands, tenant organizations, assigned or visiting DoD personnel (including military members, civilian, and contractor employees, and dependents), and how that process supports the implementation of appropriate force protection measures to protect military personnel, DoD civilians and family members.

3.6.1.1.2. Physical Security. Within a physical security context, the assessment will determine the assessed unit's ability to protect personnel by detecting or deterring terrorists, and failing that, to protect by delaying or defending against acts of terrorism. Physical security techniques include procedural measures such as perimeter security, security force training, security surveys, and armed response to warning or detection as well as physical security measures such as fences, lights, intrusion detection devices, access control systems, closed circuit television cameras, personnel and vehicle barriers, and other security systems. The assessment should also consider commercial off-the-shelf AT/FP technology enhancements and potential solutions for those circumstances where existing technology or procedural modifications do not provide satisfactory solutions.

3.6.1.1.3. Vulnerability and Response to a Threat. The assessment will examine the assessed unit's ability to determine its vulnerabilities against commonly used terrorist weapons and explosive devices along with the vulnerability to terrorist use of weapons of mass destruction. The assessment will further examine the ability to provide structural or infrastructure protection against terrorist events. The ability to respond to a terrorist event, with emphasis on a mass casualty situation, will also be examined.

3.6.1.1.4. Force Protection Plans and Programs. The assessment will examine the assessed unit's AT/FP program and ability to accomplish appropriate standards contained in DoD Instruction 2000.16, this Air Force Instruction, as well as applicable prescriptive standards established by the appropriate Combatant Command, Service, or DoD agency.

3.6.1.1.4.1. The assessment will examine written plans in the areas of counterintelligence, law enforcement liaison, intelligence support, security and post-incident response (the ability of the activity to respond to a terrorist incident, especially a mass casualty event).

3.6.1.1.4.1.1. The assessment will focus on the most probable terrorist threat for the facility and appropriate countermeasures. In cases where no identified threat

exists, units will be assessed on their ability to implement force protection measures under increasing threat conditions in response to an increased terrorist threat level or terrorist threat warning.

3.6.1.1.4.1.2. The assessment will examine the availability of resources to support plans as written and the frequency and extent to which plans have been exercised.

3.6.1.1.4.1.3. The assessment will examine the degree to which plans complement one another and support the assessed unit's ability to identify changes in the terrorist threat, react to threat changes by implementing appropriate force protection measures and provide an appropriate response should a terrorist event occur.

3.6.1.1.5. Host Nation, Local Community, Inter-Service and Tenant Support. The assessment will examine the level and adequacy of support available to the activity from the host nation, or local community, MAJCOM, HQ USAF, and where appropriate, inter-service and tenant organizations to enhance force protection measures or respond to a terrorist incident.

3.6.1.1.5.1. The assessment will determine the integration and feasibility of plans with the host nation, local community, MAJCOM, HQ USAF and inter-service and tenant organizations to provide security, law enforcement, fire, medical and emergency response capability in reaction to a terrorist event with emphasis on mass casualty situations.

3.6.1.1.5.2. The assessment will determine the adequacy of resources available to execute agreements and the extent and frequency to which plans have been exercised.

3.6.1.1.5.3. The assessment will determine the status of formal agreements with supporting organizations via Memorandums of Understanding or Agreement, Inter-Service Support Agreements and Host Tenant Support Agreements or other methods.

3.6.1.1.6. Activity Specific Characteristics. Site specific circumstances may require assessment of additional functional areas. These additional requirements will be as directed by the Combatant Command, Service, DoD Agency or MAJCOM creating the team and should be based on site specific characteristics such as threat level, terrorist characteristics, geography and security environment.

3.6.2. Team Composition and Level of Expertise. As a minimum, the level of expertise and team composition must support assessment of the functional areas described above. Team membership will have expertise in the following areas: physical security; civil, electrical or structural engineering; special operations; operational readiness; law enforcement and operations; infrastructure; and intelligence/counterintelligence. In exceptional cases, commanders may be required to tailor team composition and scope of the assessment to meet unique requirements of a particular activity, but must meet the intent of providing a comprehensive assessment.

3.6.2.1. Specific size and certification of expertise will be as directed by the Combatant Command, Service, DoD Agency, or MAJCOM creating the team. However, team members must be functionally oriented and have experience in the assessment area to be considered for team membership.

3.6.2.2. Based on site specific factors such as threat level, terrorist characteristics, geography and security environment, assessment teams may be augmented by personnel with expertise in

the areas of linguistics; chemical, biological, radiological weapons effects; AT/FP technology; explosive ordnance disposal; special warfare; communications; information assurance or operations; and other specialties as determined by the Combatant Command, Service, DoD Agency or MAJCOM sponsoring the assessment.

3.6.3. Installation commanders will work with their parent MAJCOM to ensure their installation receives such an assessment every three years as a maximum, or as specified by the CINC for the AOR in which they reside.

**3.6.3. (AFRC)** HQ AFRC/SF schedules JSIVA, AF and AFRC vulnerability assessments of AFRC installations through HQ USAF/XOFP. Coordinate schedule will with the HQ AFRC/IG Gatekeeper, the respective installation commander, and appropriate NAF/CC and SF.

3.6.4. HQ AFSFC will disseminate lessons learned, trends, and best practices to MAJCOMs for further dissemination. MAJCOMs will develop a system to track vulnerability findings to ensure findings receive appropriate levels of funding priority.

**3.6.4. (AFRC)** HQ AFRC/SF is the lead agency to track lessons learned, trends, and best practices; and in coordination with the AFRC Force Protection Board, prioritize projects and program funding.

3.6.5. Standard 6 vulnerability assessments will be accomplished by JSIVA, Air Force, or MAJCOM vulnerability assessment teams. Each of these programs can conduct independent or joint assessments. The Air Force VAT can also conduct "over-the-shoulder" observations of MAJCOM assessments, and conduct other assessments as directed by AF/XOF or the Air Staff FPWG. MAJCOMs will provide a copy of their assessment schedule to AF/XOFP by 15 September annually.

**3.6.5. (AFRC)** Vulnerability assessments (VA) are conducted on AFRC installations by the AFRC, AF, or JSIVA team every 3 years. VAs must ensure all tenant organizations (on the installation or remote but administratively attached) are integrated into the force protection plan and afforded the same level of FP support as AFRC units. AFRC vulnerability assessments are not required to physically assess every single activity on the installation, but instead must assess an appropriate number that will indicate a prudent level of FP is in place for the entire installation.

**3.6.5.1. (Added-AFRC)** The AFRC VAT will plan to conduct assessments of all AFRC installations. Where this is not possible, coordinate with the JSIVA or HQ USAF/XOFP to provide assistance. **NOTE:** At installations where AFRC is the host, AFRC conducts an assessment of the entire installation. At installations where AFRC is the tenant, the host unit's MAJCOM conducts an assessment of the entire installation to include AFRC assets.

**3.6.5.2. (Added-AFRC)** AFRC VAT composition may vary based on the type installation being assessed. The assessment team consists of a team chief (SF lead), force protection specialist (two), structural/infrastructure engineer, civil engineer readiness specialist, medical readiness specialist, explosive ordnance disposal specialist, and a terrorist options specialist. Other functional experts may augment the team as needed. Augmentation depends on type of assessment required, the nature of the installation's mission, the terrorist threat level, and the THREATCON. Assessments may require expertise in linguistics, chemical/biological/radiological weapons effects, emerging AT/FP technology, information operations (IO), special warfare, or other specialties as determined by the commander or directed by HQ AFRC/SF. Regardless of team composition, the team must have expertise in these areas:

**3.6.5.2.1. (ADDED-AFRC)** Physical Security.

**3.6.5.2.2. (ADDED-AFRC)** Structural Engineering (Weapons Effect Specialist)

**3.6.5.2.3. (ADDED-AFRC)** Operational Readiness.

**3.6.5.2.4. (ADDED-AFRC)** Security Forces Operations.

**3.6.5.2.5. (ADDED-AFRC)** Infrastructure Engineering.

**3.6.5.2.6. (ADDED-AFRC)** Counterintelligence/Intelligence.

3.6.6. Joint Staff Integrated Vulnerability Assessments provided by the Defense Threat Reduction Agency or other higher headquarters assessments meeting the proper DoD criteria can be considered a higher level review of the installation's AT/FP program for meeting the three year requirement.

**3.6.7. (Added-AFRC)** Installation commanders must make every attempt to correct AT/FP vulnerabilities identified during DoD Standards 6 and 14 vulnerability assessments; especially those that are procedural or low cost and would improve the AT/FP posture. Conversely, high cost improvements must be reviewed in context with threat and risk assessment, planned for, and programmed.

3.7. DoD Standard 7 – Application of DoD Terrorism Threat Analysis Methodology. Commanders shall use the DoD Terrorism Threat Level classification system to identify the terrorism threat in a specific overseas country.

3.7.1. The DoD Terrorism Threat Level classification system is a set of standardized terms used to quantify the level of terrorism threat on a country-by-country basis. The threat level terms are Negligible, Low, Medium, High, and Critical. The system evaluates the threat using the following threat analysis factors: existence of a terrorist group, history, capability, intentions, targeting, and security environment per DoD O-2000.12-H.

3.7.2. The Defense Intelligence Agency (DIA) sets the DoD general terrorism threat level identifying the potential risk to U.S. personnel in a particular country. The DoD threat level applies whether or not U.S. personnel are present in the country. CINCs, with geographic responsibilities, may also set terrorism threat levels for personnel, units, and installations in countries within the CINC's area of responsibility. Commanders shall use their threat analysis as the basis for developing plans and programs to protect assets within their AOR. Threat levels are estimates with no direct relationship to specific threat conditions (THREATCONS) or Defense Readiness States (DEFCONS). Threat levels must not be confused with threat conditions.

3.7.3. Effective application of the Terrorism Threat Level classification system requires an integrated terrorism threat analysis, incorporating information collection and analysis from all sources, coupled with a thorough understanding of the six threat analysis factors. Threat analysis factors must be viewed in the context of the specific security environment pertaining to individuals, deployed units, facilities and installations resident in the country being analyzed. An integrated terrorism threat assessment uses information on terrorist existence, history, capability, targeting, intentions, and security environment to understanding the details of individual, unit, facility, and installation vulnerability to a specific form of terrorist attack.

3.7.4. Air Force Intelligence (AF/XOI) and HQ AFOSI will employ the DoD terrorism threat level classification system outlined in the DoD standard in assessing and reporting the terrorist threat to USAF installations and personnel.

3.8. DoD Standard 8 – Threat Information Analysis. Commanders shall task the appropriate organizations under their command to gather, analyze, and disseminate terrorism threat information as appropriate.

3.8.1. Identifying the potential terrorism threats to DoD personnel and assets is the first step in developing an effective AT/FP program. Commanders at all levels who understand the threat can assess their ability to prevent, survive, and respond to an attack.

3.8.2. A thorough threat assessment requires the analysis of all available information on terrorist activities. In addition to tasking appropriate agencies to collect information, commanders at all levels shall ensure that personnel under their command properly report information on individuals, events, or situations that could pose a threat to the security of DoD personnel and resources.

3.8.2.1. HQ AFOSI has primary responsibility for collection, analysis, dissemination and production of terrorist threat information gathered from local authorities and counterintelligence sources.

**3.8.2.1. (AFRC)** AFRC Installation commanders maintain close liaison with the AFOSI office servicing their respective installations.

3.8.2.2. Headquarters Air Force Directorate of Intelligence, Surveillance and Reconnaissance (AF/XOI) is responsible for ensuring the timely collection, processing, analysis, production and dissemination of foreign intelligence, current intelligence, and national-level intelligence information concerning terrorist activities, terrorist organizations and force protection issues. These efforts will focus on, but will not be limited to, transnational and state-sponsored entities and organizations.

3.8.3. Headquarters Air Force Office of Special Investigations (HQ AFOSI):

3.8.3.1. Maintains counterintelligence (CI) data on terrorist activities affecting USAF or DoD resources.

3.8.3.2. Analyzes, studies, and assesses terrorist threats to Air Force personnel and resources for the Air Staff, commanders, and security planners.

3.8.3.3. Disseminates the AFOSI Quarterly Threat Assessment Update for use in localized AT awareness briefings and in pre-departure travel briefings.

3.9. DoD Standard 9 – Terrorism Threat Assessment Plan. Commanders shall prepare a terrorism threat assessment plan for their areas of responsibility.

3.9.1. CINC/Service/Agencies shall designate which subordinate commanders will prepare these assessment plans. This normally applies to installation commanders and above.

3.9.2. The terrorism threat assessment is the tool which commanders use to arrive at a judgment of risk and consequences of terrorist attack. Commanders will integrate threat information prepared by the intelligence community, technical information from security and engineering planners, and information from other sources to prepare their assessments. Terrorism threat

assessment shall be the basis and justification for recommendations on force protection enhancements, program/budget requests, and the establishment of THREATCONS.

**3.9.2. (AFRC)** Use the Demography, Symbolism, History, Accessibility, Recognizability, Population, and Proximity (DSHARPP) methodology (attachment 6) to determine the risk associated with the threat to the installation.

3.9.3. Installation Commanders will prepare a local threat assessment plan as part of overall AT/FP planning efforts. These plans will include a threat assessment of terrorism use of weapons of mass destruction.

**3.9.3. (AFRC)** AFRC Installation commanders will ensure terrorist threat assessments for their area of responsibility are incorporated in the risk assessment development process and may be included as a separate annex to the installation security plan (ISP).

3.9.3.1. AFOSI will assist installation commanders in the preparation and dissemination of terrorist threat assessments for all Air Force installations and facilities at least annually and as required by changes to the threat.

3.9.3.2. AFOSI will assist installation commanders with terrorism threat assessments in support of Air Force units deploying to locations overseas and provide them to the unit prior to departure.

3.9.3.3. Local threat assessments will be provided by the servicing AFOSI unit and country threat assessments will be provided by the AFOSI Region servicing the AF component for the affected CINC.

3.10. DoD Standard 10 – Threat Information Flow. Commanders at all levels shall forward throughout the chain of command all information pertaining to terrorist threats, or acts of terrorism involving DoD personnel or assets in their AOR.

3.10.1. The pattern of terrorist surveillance, targeting and planning is best recognized through sharing of information. These efforts shall include the chain of command and the interagency process at the appropriate level.

3.10.2. CINC/Service/Agencies shall designate which subordinate commanders shall coordinate with appropriate government agencies. This ensures awareness of terrorism threat information available through agencies such as the FBI, local law enforcement, and the Regional Security Officer in American embassies.

3.10.3. Installation commanders will establish working groups to address the threat and advise on AT/FP programs. The Threat Working Group will, as a minimum, consist of AFOSI, IN and SF. The larger working group will consist of CE, FM, JA, SG, DO, SC, and other agencies as determined by the installation commander. This group will serve as primary advisors to the commander on AT/FP policy, countermeasures and resource management in response to the assessed terrorist threat. This requirement may be fulfilled through the enhancement of the Installation Security Council and Resource Protection Executive Committee (may meet concurrently) to function as an overall Force Protection Working Group (FPWG).

**3.10.3. (AFRC)** All AFRC installations will establish and maintain an active Threat Working Group (TWG) which will meet, as a minimum, on a monthly basis and as situations warrant due to increased threat. Installation TWGs are strongly encouraged to invite their local civilian law

enforcement agencies that have legal jurisdiction over their installation. AFRC units which are tenant on active duty bases will actively seek membership with the host's TWG. The installation TWG will conduct a review of future deployments of personnel and aircraft to ensure proper AT/FP training and security measures are being implemented. Additionally, installation TWGs should review and analyze local threat data. All AFRC units review the HQ AFRC TWG weekly deployment advisory message to ensure compliance with AT/FP measures.

**3.10.3.1. (Added-AFRC)** HQ AFRC Threat Working Group (TWG) Charter. HQ AFRC/DOI chairs the TWG. Primary members are DOOM, SFOF, and AFOSI. Other staff offices may participate as required. The TWG meets as often as required but not less than once weekly.

3.10.4. The servicing AFOSI organization for the installation is the primary focal point with the Air Force for the collection and reporting of terrorist threat information gathered as the result of counterintelligence and law enforcement activities to include liaison with domestic and host nation security, law enforcement, and counterintelligence agencies.

3.10.5. Commanders at all echelons will develop procedures to ensure the immediate dissemination of threat changes to all personnel and, as appropriate, supporting law enforcement agencies.

3.11. DoD Standard 11 – Development of THREATCONS. Commanders at all levels shall develop a process, based on terrorism threat information and/or guidance from higher headquarters, to raise or lower THREATCON levels. The process shall be tailored to the local mission while allowing for higher headquarters downward directed implementation and comply with the guidance contained in DoD O-2000.12-H.

3.12. DoD Standard 12 – Coordination of THREATCON Measures Implementation. CINC/Service/Agencies ensure that THREATCON transition procedures and measures are properly disseminated and implemented by subordinate commanders within their AOR.

3.12.1. MAJCOMs and installation commanders will ensure THREATCON measures within their AORs are properly coordinated with other CINCs/Services/Agencies.

3.12.2. Tenant units, regardless of MAJCOM or service component, will conform to the host installation's THREATCON.

**3.12.2. (AFRC)** AFRC Installation commanders decide when to go to higher THREATCONS based on local conditions. Downward directed THREATCON changes for AFRC units will come from or through AFRC/CC. Tenants on AFRC bases should coordinate with owning MAJCOM/service THREATCON changes and seek concurrence from the host prior to implementing the THREATCON. AFRC Installation commanders consider the request, determine local threats, and make a base-wide determination. In those instances where local threats are absent, commanders seek clarification from AFRC prior to increasing THREATCONS. There will only be one THREATCON on AFRC bases, with final determination made by the installation commander.

3.12.3. All agencies report THREATCON changes per AFMAN 10-206, Operational Reporting. MAJCOM/SFs and FOAs assess and relay the THREATCON status to their assigned units and HQ AFSFC/SFO Operations Center.

**3.12.3. (AFRC)** All AFRC installations will immediately notify the AFRC command post upon any change in the local THREATCON.

3.13. DoD Standard 13 – Local Terrorism Threat Response Measures. Commanders at all levels shall develop measures or actions for each THREATCON utilizing at least the minimum number of measures/actions enumerated for each THREATCON as listed in DoD O-2000.12-H, *Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence*. These measures will change as the threat situation increases from THREATCON NORMAL to THREATCON DELTA.

3.13.1. Commanders at all levels shall establish local measures to supplement DoD O-2000.12-H procedures to transition between THREATCONS. Whereas Terrorism Threat Levels are intelligence judgments on the likelihood of terrorist attack, THREATCONS are graduated categories of measures or actions commanders take to protect personnel and assets from attack.

3.13.1.1. Commanders at all levels may set a local THREATCON. Subordinate commanders may raise but not lower a higher level commander's THREATCON.

3.13.1.2. Installation Commanders will establish specific threat condition measures (tailored to the local mission, conditions, and the terrorist threat) developed to augment the DoD THREATCON measures, listed in [Attachment 1](#).

3.13.1.3. Installation Commanders must continuously evaluate available information about local terrorist activity to determine whether there is a terrorist threat to installation facilities or personnel. If the information warrants action, select and declare the appropriate THREATCONS. Commanders may modify locally developed optional actions of THREATCONS based on their requirements and local threats.

3.13.1.4. Installation commanders will develop and implement a Random Antiterrorism Measure (RAM) program according to DoD O-2000.12-H that will include daily implementation of a recommended minimum of three RAMs from higher THREATCONS. RAMs should be changed often to avoid predictability. RAM execution should be broad based and involve a variety of career fields and personnel.

**3.13.1.4. (AFRC)** Installations will develop and implement written local RAMs. To be effective, use RAMs in THREATCONS Normal to Delta. As a minimum, use the RAMs contained within AFI 31-210, attachment 3. Fifty-one security measures are listed for THREATCON Alpha through Delta with one measure in each THREATCON to be determined. Locally devised measures above and beyond THREATCON Charlie may be used. Locally developed measures will follow the format provided in AFI 31-210, attachment 3. In other words, list the DoD measure and supplement with additional local measures. For example, AFI 31-210, attachment 3, paragraph A3.2.2.1 depicts DoD Measure 1. Paragraphs A3.2.2.1.1 and A3.2.2.1.2 are Air Force added supplemental measures.

3.13.1.5. Installation Commanders will incorporate AT/FP measures in plans for functions such as change of commands, open houses and organized off-base activities.

3.14. DoD Standard 14 – Physical Security Vulnerability Assessments. Commanders shall prepare a terrorism physical security vulnerability assessment for facilities, installations, and operating areas within their area of responsibility. The assessment will address the broad range of physical threats to the security of personnel and assets and will be conducted at least once every three years.

**3.14. (AFRC)** Installation commanders will ensure physical security vulnerability assessments are conducted every 3 years and reports forwarded to HQ AFRC/SF. Refer to DoDO-2000-12H, *Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence*, (Appendix

C, Physical Security Survey Instrument) for guidance on how to conduct a physical security vulnerability assessment.

3.14.1. Physical security vulnerability assessments normally occur at the installation commander level and above. These assessments should consider the range of identified and projected terrorism threats against a specific location or installation personnel, facilities, and other assets. The assessment should identify vulnerabilities and solutions for enhanced protection of DoD personnel and resources.

3.14.2. Installation Commanders must conduct a physical security vulnerability assessment at least every three years for facilities, installations, and operating areas and resources under their control. They may assemble their own assessment teams or may request AFOSI to facilitate the formation of a multi-functional vulnerability assessment team (to include representatives from installation agencies such as civil engineering, security forces, intelligence, communications, medical, AFOSI, etc.). Installation commanders will forward copies to the MAJCOM to help synchronize resource allocation and advocacy.

**3.14.2. (AFRC)** The Installation Chief of Security Forces is the OPR for conducting physical security vulnerability assessments within AFRC. Include off-site activities (outside-the-fence) as part of the assessment. Conduct assessments every 3 years or when significant changes occur. Complete initial Standard 14 assessments by December 2000. As a minimum, assessment team composition includes Security Forces (lead), AFOSI, Civil Engineering, Intelligence, Medical, and Communications. A qualified representative from the wing Information Protection Office conducts the communications portion of the physical security vulnerability assessment. Results of the Information Protection Assessment Program review conducted according to AFI 33-230, *Information Protection Assessment and Assistance Program*, will supplement the physical security vulnerability assessment. Use the JSIVA checklist, the checklist provided as an attachment to DoDO 2000.12-H, and AFOSI Pamphlet 71-123, to accomplish the assessments. Classify physical security assessment vulnerability reports pursuant to the JSIVA Security Classification Guide, Jan 2000. Forward a courtesy copy of the completed DoD Standard 14 assessment to HQ AFRC/SF within 90 days after the assessment.

3.14.3. Installation Commanders will ensure vulnerability assessments address the full spectrum of threats to mission essential critical assets, utilities, facilities, food, water, etc. They will include functional experts appropriate to the location assessed and be conducted IAW DoD O-2000.12-H.

3.15. DoD Standard 15 – Physical Security and Force Protection Plan. Commanders at all levels shall develop and implement a physical security plan, as part of the AT/FP program, that incorporates facilities, equipment, trained personnel, and procedures into a comprehensive effort designed to provide maximum antiterrorism protection to personnel and assets. Where there are multiple commanders at an installation, the Installation Commander is responsible for coordinating the physical security plans for all units on the installation.

3.15.1. Physical security against terrorism threats requires an integrated approach. A well-designed physical security system is capable of performing the following functions: detection, assessment, delay, denial, notification, and response. It should include provisions for the use of physical structures, physical security equipment, security procedures, response forces and emergency measures sufficient to achieve the desired level of force protection and consequence management.

3.15.2. Commanders should review all AT/FP program plans at least annually, or when the terrorism threat level changes. This will ensure the design and implementation of the physical security portion of the antiterrorism and force protection program is consistent with local terrorism threat conditions and addresses the need for potential enhancements.

3.15.3. Installation Commanders shall incorporate AT/FP actions for the installation's AT/FP programs in installation security plans, disaster preparedness operations plans and/or resource protection plans and provide specific guidance for the installation's AT/FP program. These actions include provisions for the use of physical structures, security equipment and procedures, response forces, and emergency measures sufficient to achieve the desired level of force protection and consequence management. These plans may be combined into one overarching AT/FP plan.

**3.15.3. (AFRC)** Recommend installation commanders use the Joint Chiefs of Staff J-34 Antiterrorism Force Protection Installation Planning Template (interactive CD-ROM) when creating or updating an installation AT/FP Plan; extract data produced by the CD-ROM when writing the AT/FP Plan. When the Installation Security Plan is completed per AFRC Supplement to 31-101, *Installation Security Program*, chapter 4 (Planning Security Operations) it becomes a combined overarching AT/FP Plan.

**3.15.3.1. (Added-AFRC)** Recommend installation commanders use the Joint Chiefs of Staff J-34 Weapons of Mass Destruction Appendix (interactive CD-ROM) to the Antiterrorism Force Protection Installation Planning Template when creating the response actions of the Installation Security Plan.

3.15.4. Installation commanders implement physical security procedures to protect against terrorism by installing up-to-date physical security equipment, implementing THREATCONS, employing Random Antiterrorism Measures (RAMs), and responding to terrorist acts.

3.15.5. Copies of all plans dealing with AT/FP will be forwarded to the installation's AT/FP Officer when published.

3.16. DoD Standard 16 – Physical Security Training and Exercises. Commanders at all levels shall exercise the physical security and force protection plan and terrorism incident response plan to determine their ability to protect personnel and assets against terrorist attack and the consequences of a successful terrorist attack.

3.16.1. Installation Commanders will ensure training and exercises are conducted IAW AT/FP plans to include all THREATCON measures, evacuation/notification plans and procedures, terrorist use of weapons of mass destruction (WMD), and other key areas outlined in their installation's security plans at least semi-annually.

**3.16.1. (AFRC)** Local command authorities exercise all portions of their AT/FP plans semi-annually. Involve local off-base agencies to the greatest extent possible and encompass duty and non-duty hours. Also include all tenant activities and/or DoD elements and personnel for whom the commander has force protection responsibility.

3.17. DoD Standard 17 – Baseline Force Protection Posture. Commanders at all levels shall routinely review the effectiveness of daily physical security measures under THREATCON NORMAL.

**3.17. (AFRC)** Commanders at all levels routinely (or when the Terrorist Threat Level changes) review the effectiveness of day-to-day physical security measures under the existing THREATCON

posture. As a minimum, consider access control, patterns of population concentrations for both work and social purposes, and sensitive areas that may be lucrative targets for terrorists and criminals.

3.17.1. Employment of DoD standards contained in this instruction become more applicable as commanders prepare for and implement responses to increased THREATCON levels. However, effective THREATCON NORMAL procedures, associated daily physical security operations and effective AT/FP training programs are the foundation for successful antiterrorism efforts.

3.17.2. Installation commanders, in coordination with the installation Threat Working Group or Force Protection Working Group, will review local THREATCON measures at least semiannually to ensure the installation's daily security procedures are appropriate. Consideration will be given to the most recent vulnerability assessment, current threat assessment, and other factors when conducting this review.

3.18. DoD Standard 18 – AT/FP Guidance for Off-Installation Housing. Commanders shall ensure DoD personnel assigned to Medium, High, or Critical Terrorist Threat Level areas, and not provided on-installation or other government quarters, are furnished guidance on the selection of private residences to mitigate risk of terrorist attack. Commanders shall include coverage of private residential housing in AT/FP plans where private residential housing must be used in Medium, High, or Critical Threat areas.

3.18.1. The best protection for individuals is an awareness of the threat and the willingness to take the steps necessary to reduce threat exposure. Proper selection of private residences can help reduce vulnerability.

3.18.2. Installation commanders will develop procedures through their local AFOSI, Security Forces, and Civil Engineer Housing Flights to ensure personnel are provided guidance on housing selection in areas with Medium, High, or Critical Terrorist Threat Levels. This guidance provides information as to selection of homes to minimize the risk of terrorist acts.

3.19. DoD Standard 19 – Residential Security Assessments for Off-Installation Housing. Commanders in Medium, High, or Critical Terrorist Threat Level areas shall conduct physical security assessments of off-installation residences for permanently assigned and temporary-duty DoD personnel. Based on the assessment results, commanders will provide AT/FP recommendations to residents and facility owners, and as appropriate, recommend to appropriate authorities the construction or lease of housing on an installation or in safer areas.

3.19.1. Complete residential security assessments in medium, high, or critical threat areas as soon as personnel have identified and are entering into contract negotiations for the lease or purchase of a residence. Residences overseas are more apt to install gratis security enhancements prior to the consummation of a contract.

3.19.2. For off-installation assessments, use the same terrorism threat, risk, and vulnerability criteria as that used to assess the safety and security of occupants of other facilities or installations housing DoD personnel in the AOR.

**3.19.2. (AFRC)** AFRC Installation commanders will ensure SV and LGC coordinate with the installation AT/FP officer, AFOSI, and SF to ensure threat assessments are conducted of all off-base lodging facilities being used by personnel during TDYs or UTAs.

3.19.3. Installation commanders assigned to Negligible or Low threat areas will evaluate the need to conduct assessments of off-installation housing areas. Installation commanders will use the

process outlined in paragraph 3.14.2. to ensure proper assessment of off-installation housing, if deemed necessary.

3.20. DoD Standard 20 – AT/FP MILCON Considerations. CINC/Service/Agencies shall establish AT/FP guidelines for new construction to counterterrorism threat capabilities within the AOR.

3.20.1. The Air Force Civil Engineer (AF/ILE) will develop guidelines IAW DoD 0-2000.12-H on force protection issues for the planning, design, refurbishment and construction of Air Force installations and facilities to minimize, if not preclude, the vulnerability of Air Force personnel to terrorist attacks. At a minimum, they will meet the evolving DoD AT/FP military construction standards.

3.20.2. Developing facilities that provide a safe and secure living and working environment in potentially hostile areas shall be a primary consideration in the planning, programming, and design of Air Force facilities. Analysis conducted during the planning and programming phases will include assessing potential threats, reviewing design opportunities and constraints, and integrating protective strategies in the facility and its immediate surroundings. Installation Commanders will ensure all new construction projects and programs employ AT/FP features and meet minimum DoD AT/FP Construction Standards. The Base Civil Engineer will coordinate security requirements with the installation security forces on all facility construction and rehabilitation projects. The installation AT/FP Officer/NCO will review and provide comment for installation commander consideration on all facility construction and rehabilitation projects to ensure compliance with AT/FP criteria.

**3.20.2. (AFRC)** All Command, Control, Communications, Computers and Intelligence (C4I), headquarters, and lodging facility projects, whether new construction or major renovation, will be reviewed by HQ AFRC/SF and installation SF personnel during the initial design process to ensure force protection considerations are properly addressed. Consideration should be given to constructing a "Safe Haven" location for installation commanders in their office to be used during duress situations. Refer to the Interim Department of Defense Antiterrorism/Force Protection Construction Standard dated 16 December 1999 and DoDO-2000.12H, chapter 10.

3.21. DoD Standard 21 – Facility and Site Evaluation/Selection Criteria. Commanders shall develop a prioritized list of AT/FP factors for site selection teams. These criteria shall be used to determine if facilities either currently occupied or under consideration for occupancy by DoD personnel, can adequately protect occupants against terrorism attack.

**3.21. (AFRC)** The MAJCOM and installation TWG conducts these assessments according to paragraph 3.10.3.

3.21.1. Circumstances may require the movement of DoD personnel or assets to facilities the U.S. government has not previously used or surveyed. AT/FP standards will be the primary consideration in evaluating the suitability of these facilities for use.

3.21.2. Installation commanders will develop a prioritized list of AT/FP factors based on the current threat for site selection teams for determining suitability for use by DoD personnel. Servicing AFOSI detachment, Medical, Intelligence, Security Forces, and Civil Engineers will provide inputs into this process.

**3.21.2. (AFRC)** Refer to the Interim Department of Defense Antiterrorism/Force Protection Construction Standard dated 16 December 1999 and DoDO-2000.12H to aid in developing AT/FP factors.

3.22. DoD Standard 22 – Pre-deployment AT/FP Vulnerability Assessment. CINC/Service/Agencies shall conduct a pre-deployment AT/FP vulnerability assessment for all units prior to deployment. Commanders shall implement appropriate force protection measures to reduce risk and vulnerability.

3.22.1. Commanders shall direct AT/FP measures to be implemented that reduce risks before, during, and after deployment. Assessments and the subsequent implementation of standards must occur in a timely manner, and be incorporated in pre-deployment planning and training. Pre-deployment assessments should assist commanders in updating AOR specific training and in obtaining necessary physical security materials and equipment to implement protective measures.

3.22.2. Prior to deployment, the senior deploying commander will ensure a pre-deployment vulnerability assessment has been conducted. These assessments will include a medical member qualified to evaluate the safety and vulnerability of local food and water sources, perform an epidemiological risk assessment, evaluate local medical capabilities, perform a vector/pest risk assessment, determine adequacy of hygiene of local billeting and public facilities, and perform an environmental risk assessment. Assessments will provide the necessary background data for sizing the force protection package required to reduce the threat to Air Force personnel and assets. MAJCOMs will determine the expertise level for persons conducting these assessments.

3.22.3. Servicing AFOSI detachments will develop the capability to provide threat assessment information for any deployments to the supported installation.

3.23. DoD Standard 23 – Designation of an AT/FP Officer/NCO. CINC/Service/Agencies, shall ensure that an AT/FP Officer, responsible to the Commander for AT/FP requirements, is assigned at each installation or base, and deploying organization (e.g. battalion, ship, squadron).

3.23.1. Commanders at all levels who deploy with their unit outside the United States, and its territories, and possessions will have an AT/FP Officer/NCO or equivalent assigned as the AT/FP subject matter expert and advisor. This individual shall ensure each person within the unit is aware of the terrorism threat, and is trained to employ methods to reduce risk or mitigate the effects should an attack occur.

3.23.2. **Table 1.** outlines training requirements for the AT/FP Officer/NCO.

3.23.3. Individuals may become qualified to administer Level I training within their units using two methods:

3.23.3.1. Attending formal Level II training that is based on the core curriculum of the John F. Kennedy Special Warfare Center and School's (JFKSWCS) Antiterrorism Instructor Qualification Course, with additional instruction that reviews current AT/FP publications and identifies methods for obtaining area of operations (AOR)-specific terrorism threat analyses, updates, and warning; or

3.23.3.2. Commanders may qualify individuals who are subject matter experts and have received formal training in AT/FP individual protection (i.e., military/security police, special agents, etc. who have received specific formal training in this area). These individuals may be individually exempted by the Commander from the Level II training outlined in **Table 1.** as long as they receive the additional training that reviews current AT/FP publications and iden-

tify the method for obtaining AOR-specific updates.

3.23.4. Installation Commanders will appoint an AT/FP Officer/NCO and alternate in writing (recommended E6 or higher) to serve as the installation commander's primary advisor. Both will receive formal education at an approved Level II course. Commanders may qualify individuals who have experience, education, or training to serve as their AT/FP Officer/NCO, and may exempt them from Level II training in writing.

**3.23.4. (AFRC)** Installation placement of the AT/FP Officer and alternate at AFRC field activities is at the commander's discretion; however, commanders should consider collocating the AT/FP Officer and alternate with force protection or program protection personnel to ensure effective implementation across organizational and functional lines. The person appointed may be an officer, NCO, DoD civilian, or for those installation/sites with contracted security, a DoD contractor. Grade criteria for the AT/FP Officer and alternate should generally target military O-2/3, E-6, or DoD civilian GS-9. Based on mission need the installation/site commander may waive target grades. Once the AT/FP Officer and alternate have been designated, forward a courtesy copy of the appointment letter containing the person's name, SSN, security clearance, duty phone number and e-mail address to HQ AFRC/SF. Update appointment letters as changes occur.

3.23.4.1. Installation Commanders will ensure AT/FP Officers/NCOs maintain ready access to antiterrorism/force protection publications outlined in Attachment 1 to establish and tailor the installation AT/FP program.

**3.23.4.1. (AFRC)** Commanders are strongly encouraged to appoint in writing individuals who have experience, education, training, etc. to serve as their AT/FP Officer and alternate. Those appointed installation AT/FP Officers should attend Level II training within 90 days of appointment. If the installation commander identifies an AT/FP Officer/alternate who has past experience, education and training, the commander may exempt them from Level II training. This exemption needs to be done in writing and identified in the AT/FP appointment letter.

3.23.5. Installation Commanders will also ensure adequate numbers of Level II trained personnel to ensure proper coverage of overseas deployments.

3.24. DoD Standard 24 – General Requirement for Antiterrorism Awareness Training. CINC/Service/Agencies shall ensure that all assigned personnel receive the appropriate training for individual anti-terrorism awareness prior to deploying or traveling outside the United States, its territories and possessions. The individual's records shall be updated in accordance with DoD Component policy. Family members shall receive similar training prior to traveling outside the United States, its territories and possessions on official government orders.

3.24.1. Individual security awareness and individual force protection training are essential elements of an overall force protection program. Each individual must share in this responsibility by ensuring alertness and the application of personal protection measures.

3.24.2. The greatest loss of life inflicted by terrorist attacks on DoD personnel has resulted from improvised explosive device (IED) attacks. Therefore, training programs will include instruction on recognizing and reporting concealed IEDs (e.g. in packages and motor vehicles).

3.24.3. Family members traveling outside the United States, its territories and possessions on official business, i.e., on a permanent change of station move, should receive this training as part of their pre-departure requirements. The military member will ensure family members are aware of

this need and receive the training. Furthermore, all levels of command should encourage family members to receive AT/FP awareness training prior to any form of travel outside the United States, its territories and possessions.

3.24.4. Training and AOR updates must meet requirements of the CINC with responsibility for that country. If Threat Levels rise above low in the Continental United States or its territories or possessions, Level I training is required.

3.24.5. **Table 1.** below describes training required by this standard.

**Table 1. PRE-DEPLOYMENT & CAREER DEVELOPMENT AT/FP TRAINING REQUIREMENTS**

Level of Training	Target Audience	Minimum Training Standard
<p>Level I (for all Threat Levels)</p> <p><u>Awareness training-</u> Conducted within six months prior To travel and delivered by a qualified instructor.</p>	<p>Military, DoD Civilians, and their family members (When family members are deploying or traveling on government orders)</p>	<ol style="list-style-type: none"> <li>1. Viewing a Service/Agency-selected personal awareness video.</li> <li>2. Issuance of JS Guide 5260 "Service Member's Personal Protection Guide: A Self-Help Handbook to Combating Terrorism" and "Antiterrorism Individual Protective Measures" folding card. (Local reproduction of both is authorized.)</li> <li>3. A USAF standardized program of instruction (POI) with the following minimum topics: Introduction to Terrorism, Terrorist Operations, Individual Protective Measures, Terrorist Surveillance Techniques, Hostage Survival, Threat Levels and THREATCON Systems.</li> <li>4. Receive AOR updates for area of travel to include current threat brief and AOR specific requirements as provided by the CINC.</li> </ol>
<p>Level II AT/FP Officer</p>	<p>AT/FP Officers/non-commissioned officers, or equivalent, who are then qualified to serve as the AT/FP advisor to the Commander and provide Level I instruction.</p>	<p>Instruction provided by a USAF approved source with:</p> <ol style="list-style-type: none"> <li>1. POI based on core curriculum of the JFKSWCS Antiterrorism Instructor Qualification Course: Introduction to Terrorism, Terrorist Operations, Detecting Terrorist Surveillance, Individual Protective Measures, Hostage Survival, Threat Levels and THREATCONS.</li> <li>2. Review of applicable AT/FP reference publications.</li> <li>3. Methods available for obtaining AOR-specific updates for deployment/travel area.</li> <li>4. USAF-directed modules on other aspects of AT/FP such as physical security requirements, technology updates, etc.</li> </ol> <p>Graduates have basic understanding and materials to provide Level I instruction and support their Commanders in conduct of the unit's AT/FP program and related issues.</p>

Level of Training	Target Audience	Minimum Training Standard
Level III	O-5/O-6 Commanders	Conducted in Service pre-command pipelines and in accordance with DoD 2000 series documents and AFIs. Include viewing SECDEF/CJCS AT/FP video, directive/reference review, and USAF-specific modules.
Level IV	O-6 to O-8 Commanders/personnel selected by Service/CINC/DoD Agency who are responsible for AT/FP programs or involved in AT/FP policy, planning and execution.	Executive-level seminar providing pertinent current updates, briefings, panel discussion topics. Seminar concludes with a tabletop AT/FP wargame aimed at facilitating interaction and discussion among the participants.

3.24.6. Minimum training requirements for Level I-IV training are included in Table 1.1.

3.24.7. Level I. Level I Antiterrorism Training is mandatory for all AF personnel within six months of any deployment, leave, or travel outside the continental US. For those individuals going PCS, the MPF Outbound Assignment Checklist will include this training requirement to their relocation processing letter and must be completed prior to final out-processing. For those individuals going TDY, the Unit Deployment Managers (UDMs) are required to ensure all individuals receive this training prior to deployment. AFOSI special agents and other Level II trained personnel may conduct Level I training. Unit ancillary training managers will document Level I training in PC-III annotating that training was conducted and the date of completion. HQ AFOSI and HQ AFSFC/SFP jointly develop antiterrorism awareness briefings for use in delivering Level I training. Level I training offered by other services or DoD agencies meets DoD requirements as long as all requirements listed in Table 1 are fulfilled.

**3.24.7. (AFRC)** Unit training managers will annotate dates of completion of AT/FP Level 1 Training in PC-III when the PC-III system has been updated to accept this information. Unit commanders of personnel deploying to overseas locations will ensure annotation of this training on the individual's travel orders and/or instruct them to hand-carry a copy of the PC-III print-out which indicates training has been completed.

3.24.8. Installation commanders will:

3.24.8.1. Develop procedures to ensure all military and civilian personnel traveling overseas TDY, PCS, or on leave, including family members and DoD contract personnel on official travel, receive Level I Antiterrorism Awareness Training and that this training is properly documented.

**3.24.8.1. (AFRC)** Commanders will develop written procedures to ensure proof of Level I training is part of the TDY order/leave authenticating process. Personnel who have not completed Level I AT/FP training with special emphasis on AOR-specific threat and medical threats will not be issued orders for overseas travel (deployed, TDY or leave). The Joint Staff Guide 5260 is available via GCCS on the J-34 Combating Terrorism web site <http://nmcc20a.nmcc.smil.mil/~dj3cleap/j34pubsdocs/j34/pubsdoc.html>. Local reproduction is authorized.

3.24.8.2. Ensure anyone traveling to DoD-designated high-threat areas as defined in the Foreign Clearance Guide is briefed on the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (OASD (SO/LIC)) or USAF/ILT DoD Travel Security Advisories, and any Federal Aviation Administration (FAA) travel advisories.

3.24.8.3. Receiving installation commanders will report the following information through their MAJCOM assignments or deployments representative to HQ AFSFC/SFP quarterly for all personnel who arrive without Level I training: Full Name, Rank, Sending Unit, Sending MAJCOM, Receiving Unit, Receiving MAJCOM, total number of gains for the period.

3.24.8.4. Ensure all personnel receive annual force protection training. The depth of this training is determined by the MAJCOM and may be accomplished through video, computer based training, or other means. This training must be documented by the unit training monitor.

**3.24.8.4. (AFRC)** Commanders and directorate heads must ensure their personnel receive annual force protection training. The DoD AT/FP video "You May Be the Target" is the tool used to conduct the annual force protection training. Use this IP address <http://dodimagery.afis.osd.mil> to order the video. Document force protection training in the same manner as other ancillary training. Training documentation is subject for review during vulnerability assessments conducted pursuant to DoD Standards 6 and 14.

3.24.9. Level II training is designed for individual qualification for those assigned as the installation AT/FP Officer/NCO. This course also serves as the primary venue for training AT/FP representatives that deploy forward. Each installation and deploying AT/FP Officer/NCO will attend Level II training. Level II graduates can also provide Level I training. Each installation requiring Level II training for their assigned AT/FP officer or other personnel as needed will schedule training through their MAJCOM/SF. Level II training is open to all AFSCs.

**3.24.9. (AFRC)** Units needing Level II training schedule the requirement with HQ AFRC/SFOF. Personnel selected to attend the Level II course must be prioritized as follows: installation AT/FP Officer and alternate, key leadership assigned to UTCs, and other specialties on the installation key to successful UTC deployment; i.e., combat logistics, communications, prime beef, medical personnel and other unique teams. Submit prioritized Level II training requests to HQ AFRC/SFOF under wing commander or equivalent signature. Requests must include full name, rank/grade, SSN, security clearance, and duty phone to facilitate the request.

3.24.9.1. MAJCOMs who desire to establish their own Level II training programs will coordinate their programs with HQ AFSFC/SFP prior to initiating any training. All Air Force Level II programs will use a standardized curriculum based on the JFKSWCS Course. Instructors must be graduates of the Antiterrorism Instructor Qualification Course (AIQC) or another course of instruction, including other Services courses, approved by HQ AFSFC/SFP. MAJCOMs may add command-specific requirements to the core curriculum.

**3.24.9.1. (AFRC)** All AFRC AT/FP Level II Mobile Training Team (MTT) instructors will be certified by HQ AFRC/SF prior to instructing any AFRC classes. HQ AFRC/SFOF establishes an AT/FP Level II instructor list of certified instructors. The AFRC AT/FP Level II MTT instructor list is made up of lead instructors and support instructors. A minimum of one lead instructor must be present to control the course of instruction during all AFRC AT/FP Level II classes. Lead instructors are graduates from the Antiterrorism Instructor Qualifica-

tion Course (AIQC). Support instructors are graduates of an AT/FP Level II course and have functional expertise in the AT/FP subject matter.

3.24.9.2. All Level II training programs will report their monthly totals of the number of personnel trained no later than the 10th day of the following month to HQ AFSFC/SFP.

3.24.10. Level III. Commander Antiterrorism Training is designed for squadron, group, and wing commanders. MAJCOM/SFs will provide this training to squadron commanders during MAJCOM squadron commander orientation seminars. Group and wing commanders will receive this education through the group and wing commanders' courses at Maxwell AFB AL.

**3.24.10. (AFRC)** HQ AFRC/SF provides Level III training during the AFRC squadron commander orientation course taught at Robins AFB GA.

3.24.11. Level IV. Executive-Level Commander Training is accomplished by the Combating Terrorism Directorate of the Joint Staff (J34). It is designed for installation commanders, JTF/Battle Group level commanders, and those responsible for AT/FP policy, planning, and execution. Once quotas for this training are established through J-34, Combating Terrorism Directorate, allocations are made through the AF General Officer Matters Office and AF Colonel Matters Office. Nominee selection will be by position, based on assignment in or to high risk locales.

3.24.12. Personal Responsibilities. All personnel must exercise proper caution to reduce vulnerability. Attachment 1 lists several references that identify measures that may reduce personal vulnerability to terrorism.

3.25. DoD Standard 25 – AOR-specific Training Requirements for all DoD Personnel. Combatant Commanders with geographic responsibilities shall ensure that all DoD personnel entering their AOR have been provided country-specific information on AT/FP.

3.25.1. Combatant Commanders with geographic responsibilities have significant responsibilities for protecting personnel within their AOR. Individuals traveling outside the United States, its territories and possessions for either permanent or temporary duty shall complete the prescribed general AT/FP awareness training and specific AOR training prior to travel. Combatant commanders will make AOR specific AT/FP information available to Military Departments, supporting CINCs, and DoD Agencies and Field Activities in support of this training. This information can be provided through multiple means including CINC publications, message and computer homepages.

3.25.2. Commanders at all levels who receive individuals that are not properly trained shall report the deficiency through the chain of command.

3.25.3. All Commanders will ensure that personnel who deploy, PCS, or travel on leave outside the CONUS receive AT/FP training with special emphasis on AOR-specific terrorist and medical threats. Commanders will develop procedures to ensure this training is conducted prior to departing home station and that AOR specific information is incorporated into their Level I training program. AOR-specific threat briefing information for the geographic CINCs can be found on the Internet & SIPRNET sites listed in Attachment 6.

**3.25.3. (AFRC)** Procedures prohibit the issuance of orders for overseas travel (deployed, PCS, TDY or leave) for those personnel who have not received Level I AT/FP training with special emphasis on AOR-specific threat and medical threats.

3.26. DoD Standard 26 – Training for High Risk Personnel and High Risk Billets. Combatant commanders with geographic responsibilities shall ensure personnel designated as personnel at high risk to terrorist attack and personnel assigned to high-risk billets receive appropriate AT/FP training prior to assuming duties.

3.26.1. CINCs have been given substantial AT/FP responsibilities for DoD personnel in their AORs assigned to high-risk billets or as personnel at high risk to terrorism attack. These individuals are eligible for advanced AT/FP training. In some instances, the training may be extended to include family members. Whenever possible, this training should be conducted by the Services prior to arrival in theater.

3.26.2. MAJCOM and FOA commanders decide if senior Air Force officials assigned to or visiting high-threat areas will be designated high-risk personnel.

3.26.3. Travel of High-Risk Personnel. When the threat dictates, commanders restrict access to the details of travel arrangements for high-risk individuals or senior officials (general officer or civilian equivalent) to reduce the vulnerability to attack. Unless these restrictions apply to issues other than travel security, this instruction will not stop public announcements of special events, guest speakers, or other ceremonies that senior officials attend. Make such announcements without divulging the specific travel itinerary or local arrangements.

3.26.4. Those responsible for itineraries of high-risk personnel (including general officers and civilian equivalents) must at least mark these detailed itineraries For Official Use Only (FOUO). Consider classifying travel itineraries as confidential when officials travel to high-threat areas. Declassify itineraries when the trip is over.

**3.26.4. (AFRC)** Executive officers, executive secretaries, and others responsible for accomplishing itineraries for general officers, AFRC installation commanders, and DAF civilian equivalents are responsible for marking travel itineraries For Official Use Only (FOUO) or classifying the itineraries confidential when required. The itinerary classified by line shall read:

**Derived From: AFI 31-210, 1 Aug 99**

**Declassify On: Completion of Trip**

3.26.5. During increased THREATCONS, residential and travel security of assigned or visiting "High Risk" personnel or other probable terrorist targets, should be increased to counter the threat level. Ensure these people receive timely security awareness briefings. For the most serious cases, request protective services from AFOSI. Coordinate protective service requests with the unified command in cases where, due to host country policy, AFOSI protection is not allowed.

3.26.6. Mark travel and billeting arrangements which include the dates, times, and locations for distinguished visitors, senior officers and civilian equivalents as FOUO.

3.27. DoD Standard 27 – Training for Hostage and Kidnap Situations. Commanders shall ensure DoD personnel and dependents assigned to Medium and High Threat locations are given guidance, at least annually, on appropriate conduct in the event they are taken hostage or kidnapped.

3.28. DoD Standard 28 – Terrorism Incident Response Plan. Installation commanders shall prepare installation-wide terrorism incident response plans. These plans shall include procedures for determining the nature and scope of post-incident response measures, and plans to reconstitute the installation's ability to perform AT/FP measures.

**3.28. (AFRC)** Strongly encourage Terrorism Incident Response Plans be added to the installation security plan or the installation AT/FP plan.

3.28.1. Response plans should address the full scope of an installation's response to a terrorism incident. The nature of the response depends on many factors. The character of operations underway at the time of the terrorist incident will have significant bearing on the scope, magnitude, and intensity of response.

3.28.2. Response plans should include emergency response and disaster planning/ consequence management for installation/base engineering, security, logistics, medical, mass casualty response, transportation, personnel administration, and local/host nation support. In addition, special circumstances imposed by the nature of a terrorist attack may require broader analyses to include higher levels of authority or command. A terrorist attack on DoD installations requires immediate, close coordination with higher command.

3.28.3. Installation Commanders ensure the installation can respond to a terrorist attack through the preparation of an installation-wide terrorism incident response plan or as an annex in existing plans. This plan/annex will include procedures for determining the nature and scope of post-incident response measures, plans to reconstitute the installation's ability to perform AT/FP measures, handling mass casualties, and other areas as outlined in the DoD Standard. Response measures to incidents involving nuclear, biological, chemical material should be placed in an Annex to the Installation Disaster Preparedness Operations Plan, OPLAN 32-1, which may be a sub-portion of the overall installation AT/FP plan. This plan will be exercised at least annually.

**3.28.3. (AFRC)** As a part of the response plan, commanders are encouraged to develop a set of recognizable alarms for potential emergencies. Each alarm should have its own set of reactions and a means to immediately sound the alarm. Commanders should conduct frequent drills to familiarize all personnel with individual responsibilities during a potential emergency.

3.29. DoD Standard 29 – Inclusion of Off-Installation Personnel in Terrorism Incident Response Plans. Commanders shall ensure Terrorism Incident Response plans contain current residential location information for all DoD personnel and their dependents assigned to Medium, High, or Critical Terrorism Threat Level areas. Such plans provide for enhanced security measures and/or possible evacuation of DoD personnel and their dependents.

3.29.1. Commanders in Medium, High or Critical Terrorism Threat Level areas may need to include special security arrangements to protect DoD personnel and their dependents living on the civilian economy. Close coordination with other U.S. Government agencies and host nation is essential to ensure effective allocation of security resources and protection of DoD personnel.

3.29.2. Installation commanders in Medium or higher threat level areas will ensure terrorism incident response plans include the current residential locations and the capability to notify all DoD personnel and their dependents of changes to the terrorist threat impacting personal safety. These plans include measures to provide improved security, relocate off base personnel onto the installation, or other measures to cope with a change in the threat.

3.30. DoD Standard 30 – Executive Protection and Protective Services. Commanders shall be familiar with treaty, statutory, policy, regulatory, and local constraints on the application of supplemental security measures for certain high-ranking DoD officers who are entitled to additional protection as a result of his or her position. Commanders shall take measures necessary to provide appropriate pro-

protective services for such individuals in high-risk billets and personnel in their AOR. Review and revalidation of protective services will occur on at least an annual basis.

3.30.1. Commanders should ensure individuals requesting supplemental security measures are aware of constraints and understand their individual responsibilities in accepting additional security measures. Commanders should ensure individuals receiving supplemental security measures have completed AT/FP training, are cleared for assignment to billets, facilities, or countries requiring such protection, and have been thoroughly briefed on the duties of protective service personnel.

3.30.2. Reviews of supplemental security needs should be undertaken within 30 days of a change in the terrorist threat level assigned to an AOR containing high-risk billets or to which high-risk personnel have been assigned.

3.30.3. HQ AFOSI provides special AT/FP training including the Protective Service Operation/AT/FP Training Course, Senior Officer Security Seminar, and defensive driving courses. AFOSI also provides security advisory services and protective service operations for designated high-risk personnel based on threat.

**3.30.3. (AFRC)** Installation commanders consult with their servicing AFOSI detachment if executive protection and protective services are needed.

3.31. DoD Standard 31 – Potential Threat of Terrorist Use of Weapons of Mass Destruction. CINCs/Services/Agencies shall develop estimates for potential terrorist use of Weapons of Mass Destruction (WMD) in their AORs. Reports through the chain of command will be processed immediately when significant information is obtained identifying organizations with WMD capabilities operating in their AOR.

3.31.1. AF/XOI and HQ AFOSI collect, assess, and disseminate intelligence estimates pertaining to the potential terrorist use of WMD, as referenced in DoD O-2000.12-H, guidelines for WMD, Chapter 20. Installation commanders will incorporate any threat information regarding terrorist use of weapons of mass destruction into their installation's threat assessment plan.

**3.31.1. (AFRC)** Installation commanders task the appropriate intelligence/counterintelligence organization under their command to collect, analyze, and disseminate terrorist threat information pertaining to the potential terrorist use of WMD. Commanders at all levels ensure personnel under their command properly report information on events or situations that could pose a threat to the security of DoD personnel and resources.

3.32. DoD Standard 32 – Vulnerability Assessments for Terrorist Use of WMD. Commanders shall assess the vulnerability of installations, facilities, and personnel within their AOR to terrorist use of WMD. Such assessments address potential use of chemical, biological or radiological agents.

3.32.1. Installation Commanders will ensure potential terrorist use of weapons of mass destruction is part of their vulnerability assessment in accordance with Standard 14 of this instruction, developed with supporting base agencies, such as civil engineering, readiness, medical, etc.

**3.32.1. (AFRC)** As a minimum, assessments should include information from intelligence, logistics, medical, physical security, facility engineering, meteorological, explosive ordnance disposal, and NBC staff elements. The entire range of potential terrorist WMD use should be considered when conducting assessments. Threats from commercial chemical, biological, nuclear, and radio-

logical sources should be included as well as traditional military agents. Examples of vulnerabilities include:

- 3.32.1.1. (ADDED-AFRC) Individual protective equipment/clothing.
- 3.32.1.2. (ADDED-AFRC) Collective protection equipment and facilities,
- 3.32.1.3. (ADDED-AFRC) Medical response and emergency services capability.
- 3.32.1.4. (ADDED-AFRC) Training of personnel.
- 3.32.1.5. (ADDED-AFRC) Physical security and protective barriers.
- 3.32.1.6. (ADDED-AFRC) Facility design and construction.
- 3.32.1.7. (ADDED-AFRC) Early warning and detection.
- 3.32.1.8. (ADDED-AFRC) Alarms and attack warning.
- 3.32.1.9. (ADDED-AFRC) Threat intelligence.
- 3.32.1.10. (ADDED-AFRC) Preventive medicine and vaccination programs,
- 3.32.1.11. (ADDED-AFRC) Sustainment operations and follow on support,
- 3.32.1.12. (ADDED-AFRC) Storage of bulk hazardous material,
- 3.32.1.13. (ADDED-AFRC) Explosive ordnance disposal response capability/availability.
- 3.32.1.14. (ADDED-AFRC) Food and water sources.

3.33. DoD Standard 33 – Mitigation of Terrorist Use of WMD. Commanders at all levels shall take appropriate measures to protect DoD personnel and reduce their vulnerability to terrorist use of WMD.

3.33.1. **Table A2.1.** associates standards from this instruction with the existing DoD O-2000.12-H. Use this handbook as guidance to implement the installation program.

3.33.2. Installation Commanders will ensure all AT/FP plans cross-reference or include disaster response force procedures contained in Disaster Preparedness Operations Plan 32-1. Ensure plans address their response/mitigation assessments to terrorist use of weapons of mass destruction. Force protection plans and terrorist incident response and recovery plans/annexes will specifically address command, control, communications between local, state, and host nation emergency assistance agencies, procedures to protect, respond to, and reduce the vulnerability of AF personnel to weapons of mass destruction. Installation plans should clearly identify command and control, first responders, and other follow-on support teams. Installation Commanders will identify long-term upgrade requirements and appropriate measures to mitigate potential threats. Installation Commanders will:

3.33.2.1. Develop estimates for potential threat use of WMD in their AOR. Reports throughout the chain of command will be generated to AFSFC/SFP when information is obtained identifying organizations with WMD capabilities operating within their AOR.

3.33.2.1. (AFRC) Send reports to HQ AFRC/SFO who, in turn, sends the information to AFSFC/SFP.

3.33.2.2. Assess the vulnerability of installations, facilities, and personnel within their AOR

to the threat of WMD use. Such assessments will address potential use of chemical, biological, or radiological agents.

3.33.2.3. Task appropriate level units for support, ensuring all organic, tenant and supported units are considered and receive copies of plans.

3.33.2.4. Take appropriate measures, including attack warning, to notify and protect personnel and reduce the vulnerability to the threat of use of WMD. Ensure plans identify responders, specific local/host nation support, ensure appropriate antibiotics and antidotes are supplied, personnel are trained, and that all personnel (including dependents) are aware of the threat and can respond accordingly.

3.33.2.5. Ensure response plans include casualty, triage, decontamination, evacuation, and tracking; site security, evidence preservation, and contamination control measures; detailed interagency support and coordination measures.

3.33.2.6. Ensure first responders and treatment personnel are designated, trained, and equipped to respond to nuclear, biological, chemical/HAZMAT incidents IAW AFI 32-4001, *Disaster Preparedness Planning and Operations* and AFI 32-4002, *HAZMAT Planning and Response Operations*.

**3.33.2.7. (Added-AFRC)** As a part of the overall installation/site AT/FP plan, commanders should address the WMD threat and exercise the WMD part of the plan to determine its effectiveness in mitigating the effects of an attack. In addition to providing crisis action and consequence management procedures, planning should include pre-attack measures and consideration for collateral damage a WMD may have on adjacent facilities and surrounding communities. Plans should provide sufficient detail to permit organizations to rapidly recognize and respond to any terrorist event using WMD. Attachment 6 provides additional crisis action planning considerations that should be included in addressing terrorist use of WMD.

MARVIIN R. ESMOND  
DCS/Air & Space Operations

## Attachment 1

## GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

*References*

DoD Directive 1300.7, *Training and Education Measures Necessary to Support the Code of Conduct*

DoD Directive 2000.12, *DoD Antiterrorism/Force Protection (AT/FP) Program*

DoD O-2000.12-H, *Protection of DoD Personnel Against Acts of Terrorism and Political Turbulence*

DoD Instruction 2000.14, *DoD Combating Terrorism Program Procedures*

DoD Instruction 2000.16, *DoD Combating Terrorism Program Standards*

DoD 5200.8-R, *Physical Security Program (C3I)*

DoD Instruction 5210.84, *Security of DoD Personnel at U.S. Missions Abroad*

**(Added-AFRC)** Interim Department of Defense Antiterrorism/Force Protection Construction Standard, 16 Dec 99

Joint Pub 1-03.30, *Joint After-Action Reporting System*

Joint Pub 3-07.2, *Joint Tactics, Techniques, and Procedures for Antiterrorism*

Joint Staff Guide 5260, *Service Member's Personal Protection Guide: A Self Help Handbook to Combating Terrorism*

Joint Staff Handbook 5260, *Commander's Handbook for Antiterrorism Readiness*

Joint Staff Guide 5260, *Coping with Violence: A Personal Protection Pamphlet*

**(Added-AFRC)** Joint Chiefs of Staff J-34 CD-ROM, *Antiterrorism Force Protection Installation Planning Template*

**(Added-AFRC)** DTRA, *Joint Staff Integrated Vulnerability Assessment Program Security Classification Guide, 1 Sep 97*

*United States Air Force Foreign Clearance Guide*

AFMAN 10-206, *Reporting Instructions*

AFH 10-222 Vol. 3, *Guide to Civil Engineer Force Protection*

**(Added-AFRC)** AFI 10-1101, *Operations Security*

AFI 13-207, *Preventing and Resisting Aircraft Piracy*

AFI 31-101, *The Air Force Physical Security Program*

AFI 31-209, *The Air Force Resources Protection Program*

AFI 32-4001, *Disaster Preparedness Planning and Operations*

AFH 32-4014, Vol. 4, *USAF Ability to Survive and Operate Procedures In A Nuclear, Biological, and Chemical (NBC) Environment*

AFH 32-4016, Vol. 1, *Civil Engineer Readiness Emergency Management Planning and Analysis Handbook*

AFMAN 32-4017, *Civil Engineer Readiness Technician's Manual for Nuclear, Biological, and Chemical Defense*

AFPD 35-1, *Public Affairs Management*

AFPD 35-2, *Public Communication Programs*

AFI 35-102, *Crisis Planning, Management and Response*

AFI 36-2202, *Managing and Conducting Military Training Programs*

AFI 36-2209, *Survival and Code of Conduct Training*

AFI 48-101, *Aerospace Medical Operations*

AFI 48-116, *Food Safety Program*

AFI 48-119, *Medical Services Environmental Quality Programs*

AFH 32-1084, *Air Force Standard Facility Requirements*

AFMAN 32-1071 (Vol. 1, 2, 3), *Security Engineering*

AFMAN 32-10138, *Military Construction Planning and Programming Manual*

AFCAT 36-2223, *USAF Formal Schools (Policies, Responsibilities, General Procedures, and Course Announcements)*

**(Added-AFRC)** AFSFC/SFP CD-ROM *Antiterrorism Reference Library*

**(Added-AFRC)** AFSFC/SFP CD-ROM *Explosive Recognition 1 and 2*

*Air Force Center for Environmental Excellence (AFCEE) Installation Force Protection Guide*

**(Added-AFRC)** *Air Force Strategic Plan, Vol. 2, Performance Plan Annex Performance Measures Details, Feb 99*

AR 525-13, *Antiterrorism Force Protection (AT/FP): Security of Personnel, Information, and Critical Resources*

MEDIC CD ROM, *Medical Environmental Disease Intelligence and Countermeasures*

*Medical Management of Biological Casualties Handbook, US Army Medical Research Institute of Infectious Diseases*

*Medical Management of Chemical Casualties Handbook, Medical Research Institute of Chemical Defense, Aberdeen Proving Ground*

*Field Management of Chemical Casualties Handbook, Chemical Casualty Care Office, Medical Research Institute of Chemical Defense, Aberdeen Proving Ground*

**(Added-AFRC)** *Chem-Bio Handbook, Janes*

### **Terms**

**Antiterrorism Program Element 28047F**—Includes manpower authorization, antiterrorism equipment, procurement, military construction, and the associated costs specifically identified and measurable to

those resources and activities associated with the Air Force Antiterrorism Program.

**Antiterrorism (AT)**—Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces. Also called AT. (Joint Pub 1-02)

**(Added-AFRC) AT Awareness**—Fundamental knowledge of the terrorist threat and measures to reduce personal vulnerability to terrorism. (Joint Pub 1-02)

**(Added-AFRC) AT Resident Training**—Formal classroom instruction in designated DoD courses that provide specialized instruction on specific combating terrorism topics; that is, personal protection, terrorism analysis, regional interest, and AT/FP planning. (DoD Directive 2000.12)

**Combating Terrorism**—Actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts) and counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism), taken to oppose terrorism throughout the entire threat spectrum. (Joint Pub 1-02)

**Counterintelligence**—Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. Also called CI. (Joint Pub 1-02)

**Counterintelligence Support**—Conducting counterintelligence activities to protect against espionage and other foreign intelligence activities, sabotage, international terrorist activities, or assassinations conducted for, or on behalf of, foreign powers, organizations, or persons. (Joint Pub 1-02)

**Counterterrorism (CT)**—Offensive measures taken to prevent, deter, and respond to terrorism. Also called CT. (Joint Pub 1-02)

**Deterrence**—The prevention from action by fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction. (Joint Pub 1-02)

**(Added-AFRC) DoD Civilian Work Force**—U.S. citizens or foreign nationals working for the Department of Defense, paid from appropriated or nonappropriated funds under permanent or temporary appointment. This includes employees filling full-time, part-time, intermittent, or on-call positions. Specifically excluded are all Government contractor employees. Contingency and emergency planning for contractor employees is covered by DoD Instructions 3020.37 and 1400.32.

**(Added-AFRC) DoD Designated High Physical Threat Countries**—Countries determined to be of significant terrorist threat to DoD travelers, as designated by the ASD (SO/LIC), in coordination with the Assistant Secretary of Defense for International Security Affairs (ASD[ISA]) and the Assistant Secretary of Defense for International Security Policy (ASD[ISP]). (DoD Directive 2000.12)

**DoD Random Antiterrorism Measures (RAM) Program**—Random, multiple security measures that consistently change the look of an installation's security program. RAMS introduce uncertainty to an installation's overall security program to defeat surveillance attempts and make it difficult for a terrorist to accurately predict our actions.

**(Added-AFRC) Domestic Terrorism**—Terrorism perpetrated by the citizens of one country against fellow countrymen. This includes acts against citizens of a second country when they are in the host country and not the principal or intended target. (DoD Directive 2000.12)

**Environmental Threat Assessment**—Multimedia medical assessment for biological, chemical,

physical, and radiological hazards at an established installation or at a deployment site.

**Force Protection Program**—Security program designed to protect Service members, civilian employees, family members, facilities, and equipment, in all locations and situations, accomplished through planned and integrated application of combating terrorism, physical security, operations security, personal protective services, and supported by intelligence, counterintelligence, and other security programs. (Joint Pub 1-02.)

**High-Risk Billet (Position)**—Authorized personnel billet (identified and recommended by appropriate authority) that because of grade, assignment, travel itinerary, or symbolic value may make those personnel filling them an especially attractive or accessible terrorist target.

**High-Risk Personnel**—Personnel who, by their grade, assignment, symbolic value, or relative isolation, are likely to be attractive or accessible terrorist targets. (Joint Pub 1-02)

**High-Risk Targets**—US material resources and facilities that, because of mission sensitivity, ease of access, isolation, and symbolic value may be an especially attractive or accessible terrorist target. Installation commanders may designate other US facilities such as clubs, base exchanges, commissaries, passenger terminals, medical facilities, and DoD schools as high-risk targets because they concentrate large numbers of US personnel. This category is for use in local planning and does not require reporting to HQ USAF.

**High-Threat Areas**—Countries, geographic regions, or transportation centers that the Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (ASD (SO/LIC)) or the regional commander in chief identifies as having significant, actual, or potential terrorist activity. This designation requires DoD individuals assigned to or traveling through the identified areas to take precautions to reduce their vulnerability to terrorism. Rapid changes in terrorism may require HQ AFOSI to designate countries as high-threat based on threats unique to the Air Force, or on intelligence information that indicates a terrorist threat. The current list of high-threat areas is in the US Air Force Foreign Clearance Guide.

**Hostage**—A person held as a pledge that certain terms or agreements be kept. (The taking of hostages is forbidden under the Geneva Conventions, 1949). (Joint Pub 1-02)

**Personal Force Health Protection**—Pre-deployment countermeasures to medical threats, provided by the commander.

**Protective Services**—AFOSI measures to increase the personal protection of dignitaries and others under the protection of the Air Force of DoD (see AFI 71-101, Vol. II).

**Terrorist Threat Assessment**—Assessments used to determine threat levels, implement security decisions, and establish awareness and training requirements. The standardized joint-service criteria are the basis for assessments used by the Chairman of the Joint Chiefs of Staff.

**Improvised Explosive Device (IED)**—A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract. It may incorporate military stores, but is normally devised from nonmilitary components. (Joint Pub 1-02)

**Installation**—A grouping of facilities, located in the same vicinity, which support particular functions. Installations may be elements of a base. (Joint Pub 1-02)

**Installation Commander**—The individual responsible for all operations performed by an installation.

(Joint Pub 1-02)

**Intelligence**—1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. (Joint Pub 1-02)

**Medical Intelligence**—That category of intelligence resulting from collection, evaluation, analysis, and interpretation of foreign medical, bio-scientific, and environmental information which is of interest to strategic planning and to military medical planning and operations for the conservation of the fighting strength of friendly forces and the formation of assessments of foreign medical capabilities in both military and civilian sectors. Also called MEDINT.

**(Added-AFRC) Military Service**—A branch of the Armed Forces of the United States, established by act of Congress, in which persons are appointed, enlisted, or inducted for military service, and which operates and is administered within a Military or Executive Department. The Military Services are the United States Army, United States Navy, United States Air Force, United States Marine Corps, and the United States Coast Guard. (Joint Pub 1-02)

**(Added-AFRC) No Double Standard Policy**—Commanders may immediately disseminate to DoD personnel and facilities information on specific terrorist threats directed against DoD personnel and facilities. However, it is the policy of the United States Government that no double standard regarding availability of information will exist. Official Americans cannot benefit from receipt of information that might equally apply to the public, but is not available to the public. Responsibility for the release of threat information to the public in CONUS remains with the FBI and overseas with the Department of State. Threats directed against or affecting the American public, or against events/locales visited/utilized by the American public, will be coordinated with the FBI or DOS, as appropriate, prior to release. This policy applies only when the information available is sufficient for DoD activities to conclude that an act of terrorism will occur and to predict, with reasonable accuracy, the time, place, mode of the attack, and, if possible, the perpetrators. When such specificity exists, but it is impossible to determine that only Government targets might be affected, it is DoD policy that the reporting entity unilaterally disseminating the information will include both DOS and the AMEMBASSY or AMEMBASSIES concerned, on the message correspondence. The “No Double Standard” requirement for commanders at all levels is simple: keep either the American Embassy or the local office of the FBI informed of your threat levels and threat conditions. This can be accomplished through direct liaison if authorized or through the CINC via the chain of command. (DoD Directive 2000.12)

**(Added-AFRC) Overseas Security Advisory Council (OSAC)**—OSAC was established by the Department of State in 1985 to foster the exchange of information between American companies with overseas operations and the U.S. Government. Government and business representatives have joined to use OSAC as a forum to produce a series of publications providing guidance, suggestions, and planning techniques on a variety of security-related issues, including terrorism.

**Physical Security**—That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material and documents; and to safeguard them against espionage, sabotage, damage, and theft. (Joint Pub 1-02)

**Proactive Measures**—In antiterrorism, measures taken in the preventive stage of antiterrorism designed to harden targets and detect actions before they occur. (Joint Pub 1-02)

**Status-of-Forces Agreement (SOFA)**—An agreement which defines the legal position of a visiting

military force deployed in the territory of a friendly state. Agreements delineating the status of visiting military forces may be bilateral or multilateral. Provisions pertaining to the status of visiting forces may be set forth in a separate agreement, or they may form a part of a more comprehensive agreement. These provisions describe how the authorities of a visiting force may control members of that force and the amenability of the force or its members to the local law or to the authority of local officials. To the extent that agreements delineate matters affecting the relations between a military force and civilian authorities and population, they may be considered as civil affairs agreements. Also called SOFA. (Joint Pub 1-02)

**Terrorism**—The calculated use of unlawful violence or threat of unlawful violence to inculcate fear. It is intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. (Joint Pub 1-02.)

**Terrorist**—An individual who uses violence, terror, and intimidation to achieve a result. (Joint Pub 1-02)

**Terrorist Groups**—Any element regardless of size or espoused cause, which repeatedly commits acts of violence or threatens violence in pursuit of its political, religious, or ideological objectives. (Joint Pub 1-02)

**Terrorist Threat Conditions**—A Chairman of the Joint Chiefs of Staff-approved program standardizing the Military Services' identification of and recommended responses to terrorist threats against US personnel and facilities. This program facilitates inter-Service coordination and support for antiterrorism activities. Also called THREATCONS. There are four THREATCONS above normal:

**THREATCON ALPHA**—This condition applies when there is a general threat of possible terrorist activity against personnel and facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of THREATCON BRAVO measures. However, it may be necessary to implement certain measures from higher THREATCONS resulting from intelligence received or as a deterrent. The measures in this THREATCON must be capable of being maintained indefinitely.

**THREATCON BRAVO**—This condition applies when an increased and more predictable threat of terrorist activity exists. The measures in this THREATCON must be capable of being maintained for weeks without causing undue hardship, affecting operational capability, and aggravating relations with local authorities.

**THREATCON CHARLIE**—This condition applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel and facilities is imminent. Implementation of measures in this THREATCON for more than a short period probably create hardship and affect the peacetime activities of the unit and its personnel.

**THREATCON DELTA**—This condition 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 likely. Normally, this THREATCON is declared as a localized condition. (Joint Pub 1-02)

**Threat Analysis**—In antiterrorism, threat analysis is a continual process of compiling and examining all available information concerning potential terrorist activities by terrorist groups that could target a facility. A threat analysis incorporates all factors of a terrorist group's existence, capability, intentions, history, and targeting, as well as the security environment within which friendly forces operate. Threat analysis is an essential step in identifying probability of terrorist attack and results in a threat assessment. (Joint Pub 1-02)

**Threat and Vulnerability Assessment**—In antiterrorism, the pairing of a facility's threat analysis and vulnerability analysis. (Joint Pub 1-02)

**Weapons Of Mass Destruction**—In arms control usage, weapons that are capable of a high order of destruction and/or of being used in such a manner as to destroy large numbers of people. Can be nuclear, chemical, biological, and radiological weapons, but excludes the means of transporting or propelling the weapon where such means is a separable and divisible part of the weapon. (Joint Pub 1-02)

## Attachment 2

## REFERENCES TO DOD O-2000.12-H

Table A2.1. AT/FP STANDARDS AND ASSOCIATED CHAPTERS/APPENDICES FROM DoD O-2000.12-H

DoD Standard	Chapter and Number	Related Appendices
1. DoD Antiterrorism and Force Protection Policy	Chapter 1, 3	
2. Development of CINC/Service/Agency standards		
3. Assignment of AT/FP Operational Responsibility	Chapter 3	
4. AT/FP Coordination in Overseas Locations	Chapter 12-14	
5. AT/FP Program Development and Implementation	Chapter 5-13 and 15, 16	C, D, E
6. Periodic Review of AT/FP Program		
7. Application of DoD Terrorist Threat Analysis Methodology	Chapter 5	
8. Threat Information Collection and Analysis	Chapter 5	C, D, E,
9. Terrorist Threat Assessment Preparation	Chapter 5	C, D, E,
10. Threat Information Flow	Chapter 5	
11. Development of Local THREATCON Levels	Chapter 5	AC
12. Coordination of THREATCON Measures	Chapter 5	AC
13. Local Terrorist Threat Response Measures	Chapter 8	F, G, I, K, L, M, O, AC
14. Physical Security Vulnerability Assessments	Chapter 6-7	C
15. Physical Security and Force Protection Plan	Chapter 7	C
16. Physical Security Training and Exercises	Chapter 7	Q, T, BB
17. Baseline Force Protection Posture	Chapter 7	
18. AT/FP Guidance for Off-Installation Housing	Chapter 11	O, P
19. Residential Security assessments for Off-Installation Housing	Chapter 10	C
20. AT/FP MILCON Considerations		
21. Facility and Site Evaluation/Selection Criteria	Chapter 10	C
22. Pre-deployment AT/FP Vulnerability Assessment	Chapter 18	
23. General Requirement for Antiterrorism Awareness Training	Chapter 12	F, I, J, K, L, M, N, O, P, Q, R, T, U, W
24. Designation of AT/FP Officer		
25. AOR-Specific Training Requirements for All DoD Personnel	Chapter 12	F, I, K, L, M, N, O, P, Q, R, T
26. Designation of High Risk Position and High Risk Billets	Chapter 13	

<b>DoD Standard</b>	<b>Chapter and Number</b>	<b>Related Appendices</b>
27. Training for Hostage and Kidnap Situations	Chapter 14	U, V
28. Terrorist Incident Response Plan	Chapter 15	BB
29. Inclusion of Off-Installation Personnel in Terrorist Incident Response Plans	Chapter 15	BB
30. Executive Protection and Protective Services	Chapter 13	G, H, N
31. Potential Threat of Terrorist use of Weapons of Mass Destruction (WMD)	Chapter 20	
32. Vulnerability Assessment for Terrorist Use of WMD	Chapter 20	
33. Mitigation of Terrorist Use of WMD	Chapter 20	

**Attachment 3****TERRORISM THREAT CONDITIONS (THREATCONS)**

**A3.1.** When used in AT plans, recommend that THREATCON measures be marked "For Official Use Only" IAW DoD Regulation 5400.7-R.

**A3.2.** The Terrorism THREATCONS listed below describe progressive levels of terrorist threats to US military facilities and personnel. As Joint Chiefs of Staff-approved terminology, these terms, definitions, and recommended security measures are intended to facilitate interservice coordination and support of US military antiterrorism and force protections activities. Selection of the appropriate response to terrorist threats AT/FP remains the responsibility of the commander having jurisdiction or control over the threatened facilities or personnel.

A3.2.1. **THREATCON NORMAL:** Commanders employ Random Antiterrorism Measures during this and all THREATCONS to enhance force protection.

A3.2.2. **THREATCON ALPHA:**

A3.2.2.1. Measure 1. At regular intervals, remind all personnel and dependents to be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers. Watch for unidentified vehicles on or in the vicinity of United States installations. Watch for abandoned parcels or suitcases and any unusual activity.

A3.2.2.1.1. Based on the threat and intelligence sources, brief appropriate personnel on the threat.

A3.2.2.1.2. Based on the threat and available intelligence, increase checks of areas from which ground or missile attacks on aircraft would likely occur.

A3.2.2.2. Measure 2. The duty officer or personnel with access to building plans as well as the plans for area evacuations must be available at all times. Key personnel should be able to seal off an area immediately. Key personnel required to implement security plans should be on-call and readily available.

A3.2.2.3. Measure 3. Secure buildings, rooms, and storage areas not in regular use.

A3.2.2.4. Measure 4. Increase security spot checks of vehicles and persons entering the installation and unclassified areas under the jurisdiction of the United States.

A3.2.2.5. Measure 5. Limit access points for vehicles and personnel commensurate with a reasonable flow of traffic.

A3.2.2.6. Measure 6. As a deterrent, apply measures 14, 15, 17, or 18 from THREATCON BRAVO either individually or in combination with each other.

A3.2.2.7. Measure 7. Review all plans, orders, personnel details, and logistics requirements related to the introduction of higher THREATCONS.

A3.2.2.8. Measure 8. Review and implement security measures for high-risk personnel as appropriate.

A3.2.2.9. Measure 9. As appropriate, consult local authorities on the threat and mutual antiterrorism measures. For example: Based on the threat and type of intelligence, brief local police of the threat, actions being taken by the installation, and request appropriate assistance. If the threat is to aircraft assets, request assistance in ensuring the anti-aircraft missile footprint area at arrival/departure runways is monitored and update as necessary.

A3.2.2.10. Measure 10. To be determined.

### **A3.3. THREATCON BRAVO:**

A3.3.1. Measure 11. Continue, or introduce, all measures listed in THREATCON ALPHA, and warn personnel of any other form of attack to be used by terrorists.

A3.3.2. Measure 12. Keep all personnel involved in implementing antiterrorism contingency plans on call.

A3.3.3. Measure 13. Check plans for implementation of the next THREATCON.

A3.3.4. Measure 14. Move cars and objects; e.g., crates and trash containers, at least 25 meters from buildings, particularly buildings of a sensitive nature. Consider centralized parking.

A3.3.5. Measure 15. Secure and regularly inspect all buildings, rooms, and storage areas not in regular use.

A3.3.6. Measure 16. At the beginning and end of each workday, as well as at other regular and frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious packages.

A3.3.7. Measure 17. Examine mail (above the regular examination process) for letter or parcel bombs.

A3.3.8. Measure 18. Check all deliveries to messes, clubs, etc. Advise dependents to check home deliveries.

A3.3.9. Measure 19. Increase surveillance of domestic accommodations, schools, messes, clubs, day care, and other soft targets to improve deterrence and defense, and to build confidence among staff and dependents.

A3.3.10. Measure 20. Make staff and dependents aware of the general situation in order to stop rumors and prevent unnecessary alarm.

A3.3.11. Measure 21. At an early stage, inform members of local security committees of actions being taken. Explain reasons for actions.

A3.3.12. Measure 22. Physically inspect visitors and randomly inspect their suitcases, parcels, and other containers. Ensure proper dignity is maintained, and if possible, ensure female visitors are inspected only by a female qualified to conduct physical inspections.

A3.3.13. Measure 23. Operate random patrols to check vehicles, people, and buildings.

A3.3.14. Measure 24. Protect off-base military personnel and military vehicles in accordance with prepared plans. Remind drivers to lock vehicles and check vehicles before entering or exiting the vehicle.

A3.3.15. Measure 25. Implement additional security measures for high-risk personnel as appropriate.

A3.3.16. Measure 26. Brief personnel who may augment guard forces on the use of deadly force. Ensure there is no misunderstanding of these instructions.

A3.3.17. Measure 27. As appropriate, consult local authorities on the threat and mutual antiterrorism measures.

A3.3.18. Measures 28-29. To be determined.

#### **A3.4. THREATCON CHARLIE:**

A3.4.1. Measure 30. Continue, or introduce, all measures listed in THREATCONS ALPHA and BRAVO.

A3.4.2. Measure 31. Keep all personnel responsible for implementing antiterrorism plans at their places of duty.

A3.4.3. Measure 32. Limit access points to the absolute minimum.

A3.4.4. Measure 33. Strictly enforce control of entry. Randomly search vehicles.

A3.4.5. Measure 34. Enforce centralized parking of vehicles away from sensitive buildings.

A3.4.6. Measure 35. Issue weapons to guards. Local orders should include specific orders on issue of ammunition.

A3.4.7. Measure 36. Increase patrolling of installation. If the threat and intelligence warrants, pay particular attention to locations where attacks against aircraft could be mounted such as parking areas and arrival departure ends of the runway.

A3.4.8. Measure 37. Protect all designated vulnerable points. Give special attention to vulnerable points outside the military establishment. Consider closing or enhancing security a remote alternate, practice, or training airfields.

A3.4.9. Measure 38. Erect barriers and obstacles to control traffic flow.

A3.4.10. Measure 39. Consult local authorities about closing public (and military) roads and facilities that might make sites more vulnerable to attacks.

A3.4.11. Measure 40. To be determined.

#### **A3.5. THREATCON DELTA:**

A3.5.1. Measure 41. Continue, or introduce, all measures listed for THREATCONS ALPHA, BRAVO and CHARLIE.

A3.5.2. Measure 42. Augment guards as necessary.

A3.5.3. Measure 43. Identify all vehicles within operational or mission support areas.

A3.5.4. Measure 44. Search all vehicles and their contents before allowing entrance to the installation.

A3.5.5. Measure 45. Control access and implement positive identification of all personnel--no exceptions.

A3.5.6. Measure 46. Search all suitcases, briefcases, packages, etc., brought into the installation.

A3.5.7. Measure 47. Control access to all areas under the jurisdiction of the United States.

A3.5.8. Measure 48. Make frequent checks of the exterior of buildings and of parking areas.

A3.5.9. Measure 49. Minimize all administrative journeys and visits. Based on the threat and intelligence, minimize aircraft departures and arrivals to operational needs.

A3.5.10. Measure 50. Coordinate the possible closing of public and military roads and facilities with local authorities.

A3.5.11. Measure 51. To be determined.

**Attachment 4****TERRORIST THREAT ASSESSMENT GUIDELINES**

**A4.1.** The purpose of this attachment is to:

A4.1.1. Establish a common terrorist threat assessment scale for use by DoD intelligence agencies.

A4.1.2. Provide commanders and other consumers of terrorist threat assessments, a definition of terrorist threat levels and a description of the factors used to assign a threat level in a given country.

**A4.2.** In assessing the terrorist threat to US personnel and interests, DoD intelligence agencies use a five-step scale to describe the severity of the threat. The following lists the threat levels and the combinations of analysis-based factors which determine the level:

A4.2.1. CRITICAL.

A4.2.2. HIGH.

A4.2.3. MEDIUM.

A4.2.4. LOW.

A4.2.5. NEGLIGIBLE.

**A4.3.** Terrorist threat levels are a product of the following six factors:

A4.3.1. Existence. A terrorist group is present, assessed to be present, or able to gain access to a given country or locale.

A4.3.2. Capability. The acquired, assessed, or demonstrated level of capability to conduct terrorist attacks.

A4.3.3. Intentions. Recent demonstrated anti-US terrorist activity, or stated or assessed intent to conduct such activity.

A4.3.4. History. Demonstrated terrorist activity over time.

A4.3.5. Targeting. Current credible information on activity indicative of preparations for specific terrorist operation.

A4.3.6. Security Environment. The internal political and security considerations that impact on the capability of terrorist elements to carry out their intentions.

**A4.4.** Threat levels are the result of combinations of the following factors based on analysis:

A4.4.1. Critical. Factors of existence, capability, and targeting must be present. History and intentions may or may not be present.

A4.4.2. High. Factors of existence, capability, history, and intentions must be present.

A4.4.3. Medium. Factors of existence, capability, and history must be present. Intentions may or may not be present.

A4.4.4. Low. Existence and capability must be present. History may or may not be present.

A4.4.5. Negligible. Existence and/or capability may or may not be present.

**NOTE:**

Security environment is considered separately as a modifying factor and AT/FP influence the assigned threat level.

**A4.5.** DoD analytic agencies may assign different threat levels to the same country. This is possible because analysts occasionally disagree about the conclusions to be drawn from the available information. Different threat levels may also be possible due to the different consumers that the individual agencies serve.

**A4.6.** Threat assessments provide information to assist commanders in determining the appropriate THREATCON. THREATCON declarations remain the exclusive responsibility of commanders. National-level DoD organizations cannot provide all intelligence that AT/FP be needed to make THREATCON determinations. Information from regional and tactical intelligence, and local law enforcement authorities must also be considered.

**A4.7.** The threat assessment scale described in this attachment applies to assessments of the terrorist threat to US and/or DoD interests only.

**A4.8.** Threat assessments are not to be confused with DoD-designated high threat areas. DoD-designated high threat areas pertain exclusively to the DoD Travel Security Policy.

**Attachment 5****AOR-SPECIFIC TRAINING**

The following links are provided for commanders, installation Force Protection Officers/NCOs, and others conducting Level I Antiterrorism Training. These sites are to be used to get the AOR update required for all overseas TDY/PCS/Leave. Unclassified sites are also provided for getting information for family members, civilian employees, etc. who do not have security clearances.

**U.S. CENTRAL COMMAND (CENTCOM)**

CLASSIFIED: [Ccj2\\_intel-s.centcom.smil.mil/jic/terrorism/summary/indextmp.htm](http://Ccj2_intel-s.centcom.smil.mil/jic/terrorism/summary/indextmp.htm)

UNCLASSIFIED: [www.centcom.mil](http://www.centcom.mil)

Scroll down to "Antiterrorism Information." There are various links to unclassified State Department databases and Defenselink.

**U.S. SOUTHERN COMMAND (SOUTHCOM)**

CLASSIFIED: 164.232.22.173

UNCLASSIFIED: Foreign Clearance Guide and the State Department Travel Advisory Page at [travel.state.gov/travel\\_warnings.html](http://travel.state.gov/travel_warnings.html)

**U.S. EUROPEAN COMMAND (EUCOM)**

CLASSIFIED: [www.eucom.smil.mil/ecsm](http://www.eucom.smil.mil/ecsm)

UNCLASSIFIED: [www.eucom.mil/hq/ecsm](http://www.eucom.mil/hq/ecsm)

Links are set up to various agencies that offer security, travel, antiterrorism/force protection information.

**U.S. ATLANTIC COMMAND (ACOM)**

CLASSIFIED: [157.224.120.250/index.htm](http://157.224.120.250/index.htm)

Click on Staff Links, click on Antiterrorism, click on Force Protection, and then pick a country. There are also links to the Defense Intelligence Agency (DIA).

UNCLASSIFIED: State Department Travel Advisory Page at [travel.state.gov/travel\\_warnings.html](http://travel.state.gov/travel_warnings.html)

**U.S. PACIFIC COMMAND (PACOM)**

CLASSIFIED: [www.hq.pacom.smil.mil](http://www.hq.pacom.smil.mil)

Antiterrorism and travel advisories can be accessed from the main page.

UNCLASSIFIED: [www.pacom.mil/homepage.htm](http://www.pacom.mil/homepage.htm)

Antiterrorism information can be accessed from the main page. Contact J232, DSN 315-477-7366, COMM (808) 477-7366 OR JICPAC, (808) 421-2362/6061/6064/6065 to obtain current threat and intelligence information.

All classified CINC Homepages can be accessed on the SIPRNET via links from the J-34 Homepage at: [nmcc20a.nmcc.smil.mil/~dj3cleap/j34.html](http://nmcc20a.nmcc.smil.mil/~dj3cleap/j34.html)

Unclassified CINC Homepages can be accessed via the DoD Antiterrorism Homepage at: [www.dtic.mil/jcs/force protection](http://www.dtic.mil/jcs/force%20protection)

Prior to travel, all service members and dependents traveling to a geographic CINC's area of responsibility (AOR) are advised to consult the Foreign Clearance Guide and the State Department Travel Advisory Homepage at [travel.state.gov/travel\\_warnings.html](http://travel.state.gov/travel_warnings.html).

Any other questions concerning threats within the AOR, DoD members should contact their unit/organization Force Protection Advisor.

**ATTACHMENT 6 (ADDED-AFRC)**

**DEMOGRAPHY, SYMBOLISM, HISTORY, ACCESSIBILITY, RECOGNIZABILITY, POPULATION, AND PROXIMITY (DSHARPP) MATRIX EXPLANATION**

**A6.1. (Added-AFRC)** The purpose of the DSHARPP 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 DSHARPP.

**A6.2. (Added-AFRC)** After developing a list of potential targets, use the DSHARPP selection factors to assist in further refining your assessment by determining the most likely (i.e., efficient, effective, and plausible) method of attack and identifying vulnerabilities to that type of attack. After the DSHARPP 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.

**A6.3. (Added-AFRC)** Demography

**A6.3.1. (Added-AFRC)** Demography focuses mainly on the threat to personnel and asks the question "who are the targets?" Depending on the ideology of the terrorist group(s), being a member of a particular demographic group can make someone (or some group) a more likely target. Therefore, when assessing points in this area, determine whether or not the group(s) have a history of or are predicted to target:

**A6.3.1.1. (Added-AFRC)** Military members.

**A6.3.1.2. (Added-AFRC)** Family members (US citizens in general).

**A6.3.1.3. (Added-AFRC)** Civilian employees of the US government (include local nationals).

**A6.3.1.4. (Added-AFRC)** Senior officers or other high-risk personnel.

**A6.3.2. (Added-AFRC)** Assess points to the target facility (scale of 1-5; 5 being worst) in this area based upon the MO of the group in targeting specific groups, and the potential for the target to be attacked based on its housing personnel of that particular group.

<b>CRITERIA</b>	<b>SCALE</b>
Facility routinely contains substantial numbers of personnel known to be targeted by the enemy	5
Contains known target group, but rarely in large concentrations	3-4
Little target value based on demographics of occupants	1-2

**A6.4. (Added-AFRC)** Symbolism. A consider whether the target represents, or is perceived by the enemy to represent, a symbol of a targeted group (e.g., symbolic of US military, religious group disfavored by the enemy, government, authority, etc.). Assess points in this area based upon the symbolic value of the target to the enemy.

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

**A6.5. (Added-AFRC) 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.

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

**A6.6. (Added-AFRC) Accessibility.** 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. This assessment entails identifying and studying critical paths that 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:

**A6.6.1. (Added-AFRC)** Infiltration from the staging base to the target area

**A6.6.2. (Added-AFRC)** Movement from the point of entry to the target or objective

**A6.6.3. (Added-AFRC)** Movement to the target's critical element

**A6.6.4. (Added-AFRC)** Exfiltration

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

**A6.7. (Added-AFRC) Recognizability.** A target's recognizability is the degree to which it can be recognized by an operational element and/or intelligence collection and reconnaissance asset under varying conditions. Weather has an obvious and significant impact on visibility (yours and the enemy's). 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.

**A6.7.1. (Added-AFRC)** Other factors that influence 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.

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 might be confused with other targets; requires training for recognition	2-3
Target cannot be recognized under any conditions -- except by experts	1

**A6.8. (Added-AFRC)** Population. What is the population relative to other potential targets? Going on the assumption the intent of the attack is to kill or injure personnel, it follows that the more densely populated an area/facility is, the more lucrative a target it makes (all other things being equal).

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

**A6.9. (Added-AFRC)** 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 enemy hold in high regard)

CRITERIA	SCALE
Target is isolated; no chance of unwanted collateral damage to protected symbols or personnel	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 in close proximity; serious injury/damage or death/total destruction of protected personnel/facilities likely	1-2

**NOTE:**

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

**A6.10. (Added-AFRC)** Add the scores across the rows to produce the DSHARPP score for that particular target to that mode of attack. The costs for compensatory measures developed to mitigate/eliminate the vulnerabilities identified is placed in the FPIM where the row for the type of facility (target) and the column for the corresponding DSHARPP score intersect.