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

***AIR FORCE INSTRUCTION 10-245***

***21 JUNE 2002***

***Operations***

# *AIR FORCE ANTITERRORISM (AT) STANDARDS*

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**NOTICE:** This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil**

---

OPR: HQ USAF/XOF (Brig Gen Shamess)
Supersedes AFI 31-210, 1 August 1999

Certified by: HQ USAF/XO (Lt Gen Wald)
Pages: 68
Distribution: F

---

This instruction implements AFPD 10-2, *Readiness*; DoDD 2000.12, *DoD Antiterrorism/Force Protection (AT/FP) Program*, April 13, 1999; DoDI 2000.16, *DoD Antiterrorism Standards,* June 14, 2001; DoD O-2000.12-H, *Protection of DoD Personnel, Activities Against Acts of Terrorism and Political Turbulence,* 19 February 1993 and Joint Pub 3-07.2, *Joint Tactics, Techniques, and Procedures for Antiterrorism,* 17 March 1998. It establishes responsibilities and guidance for the Air Force AT Program and integrates security precautions and defensive measures. This Air Force Instruction (AFI) applies to Air Force Reserve Command (AFRC) and Air National Guard (ANG) units. AFRC and ANG tenants on active Air Force installations with in place Memorandum of Agreements and Memorandum of Understanding (MOAs/MOUs) shall participate in the host installation antiterrorism/force protection (AT/FP) program. Records Disposition. Ensure that all records created by this AFI are maintained and disposed of IAW AFMAN 37-139, *Records Disposition Schedule*.

## *SUMMARY OF REVISIONS*

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

This document has changed significantly in format in order to mirror DoDI 2000.16, *DoD Antiterrorism Standards*. This AFI changes from the 31 series, Security to the 10 series, Operations. Additionally, the term antiterrorism is stressed in this document over the term force protection. It corrects administrative errors, updates references, changes format and incorporates clarifications and changes from MAJCOMs and field units. It adds Terrorist Consequence Management planning and Vulnerability Assessments (VAs) as baseline program standards. Requires installation Antiterrorism Officers (ATOs) to be qualified by attending an approved Level II course. Identifies basic ATO roles and responsibilities. Changes DoD Threat Levels and Threat Analysis factors to reflect revised Defense Intelligence Agency (DIA) terminology. It also changes Threat Conditions (THREATCONs) to Force Protection Conditions (FPCONs) and requires installations to implement all FPCON measures ordered from higher headquarters, unless granted specific relief. Adds considerations for food and water security and mail handling procedures. An AT Plan listing unit location, site-specific measures, and linked to a FPCON will be classified, as a minimum,

CONFIDENTIAL. Directs commanders to use the AFOSI local counterintelligence threat assessment as the basis for AT planning. Requires AT Plans to include procedures for using counterintelligence defensive programs locally. Requires installation Random Antiterrorism Measures (RAMs) for all FPCONs and requires at least three RAMs per day. Defines the minimum key elements required in an AT Plan. Requires installations establish detailed barrier plans. Requires reporting on AF Strategic Plan, Volume 2 Antiterrorism/Force Protection (AT/FP) Performance Measures. Requires commanders to maintain lessons learned and AT/FP exercise documentation for at least one year. Changes requirement for personnel to receive Level I AT Awareness Training. Changes requirement for area of responsibility (AOR) specific updates for personnel traveling OCONUS. Requires all Level II courses to establish Personnel Data System (PDS) Code "AFI." Requires MAJCOMs to conduct annual curriculum review of their Level II courses. RAVEN graduates, prior to Jan 2001, are awarded AT Level II credit based on the curriculum in place prior to the aforementioned date. RAVEN graduates after Jan 2001 are not authorized to perform duties as ATOs or Level I instructors, due to additional training requirements listed in DoDI 2000.16, Table 1.1, and this instruction. Establishes documentation procedures for USAF personnel who have completed Level II training offered by other Services. Changes curriculum requirements for AT Level II and Level III Training. Requires VAs be classified in accordance with the Defense Threat Reduction Agency (DTRA) VA Classification Guide. Requires local VAs be conducted annually, with the exception of the year the installation receives a higher headquarters VA. Establishes criteria for determining which DoD sites/facilities require VAs. Requires commanders to prioritize, track and report vulnerabilities identified during VAs to the next general officer/flag officer or equivalent. Adds procedures for installations receiving HQ Air Force Security Forces Center (AFSFC) VAs. Introduces the Force Protection Integrated Support Team (FIST) mission and capabilities. Adds list of approved Level II AT Courses.

**Chapter 1— AIR FORCE AT PROGRAM** **5**

1.1. Air Force AT Program. ..... 5

**Chapter 2— DoD AND AIR FORCE ESTABLISHED STANDARDS** **6**

2.1. DoD and Air Force Established Standards. ..... 6

2.2. DoD Standard 2 - Development of AT Standards. ..... 10

2.3. DoD Standard 3 - Assignment of AT Operational Responsibility. ..... 11

2.4. DoD Standard 4 - AT Coordination in Overseas Locations. ..... 12

2.5. DoD Standard 5 - Comprehensive AT Development, Implementation and Assessment. 12

2.6. DoD Standard 6 - Designation of Antiterrorism Officers (ATOs). ..... 13

2.7. DoD Standard 7 - Application of Department of Defense (DoD) Terrorism Threat Analysis Methodology. ..... 14

2.8. DoD Standard 8 - Threat Information Collection and Analysis. ..... 15

2.9. DoD Standard 9 - Threat Information Flow. ..... 16

2.10. DoD Standard 10 – Potential Threat of Terrorist Use of Weapons of Mass Destruction (WMD). ..... 16

2.11. DoD Standard 11 - Adjustment of Force Protection Conditions (FPCONs). ..... 16

2.12. DoD Standard 12 - FPCON Measures Implementation. ..... 17
2.13. DoD Standard 13 - FPCON Measures. ..... 17
2.14. DoD Standard 14 - Commanders Shall Maintain a Comprehensive AT Program for Those Personnel and Assets for Which They Have AT Responsibilities. ..... 18
2.15. DoD Standard 15 - Terrorism Threat Assessment. ..... 19
2.16. DoD Standard 16 - AT Physical Security Measures. ..... 20
2.17. DoD Standard 17 - Terrorist Incident Response Measures. ..... 21
2.18. DoD Standard 18 - Terrorist Consequence Management Measures. ..... 23
2.19. DoD Standard 19 - Training and Exercises. ..... 23
2.20. DoD Standard 20 - Comprehensive AT Review. ..... 24
2.21. DoD Standard 21 - General Requirements for AT Training. ..... 24
2.22. DoD Standard 22 - Level I AT Awareness Training. ..... 24
Table 2.1. Level I AT Awareness Training. ..... 27
2.23. DoD Standard 23 - AOR-Specific Training Requirements for all DoD Personnel. .. 27
2.24. DoD Standard 24 - Level II Antiterrorism Officer (ATO) Training. ..... 28
Table 2.2. Level II ATO Training Requirements. ..... 31
Table 2.3. Level III Pre-Command AT Training Requirements. ..... 33
Table 2.4. Level IV Executive Seminar Training Requirements. ..... 34
2.25. DoD Standard 25 - Training for High-Risk Personnel and High-Risk Billets. ..... 34
2.26. DoD Standard 26 - Vulnerability Assessment of Installations. ..... 35
2.27. DoD Standard 27 - Pre-deployment AT Vulnerability Assessment. ..... 40
2.28. DoD Standard 28 - Construction Considerations. ..... 41
2.29. DoD Standard 29 - Facility and Site Evaluation and/or Selection Criteria. ..... 42
2.30. DoD Standard 30 - AT Guidance for Off-Installation Housing. ..... 42
2.31. DoD Standard 31 - Executive Protection and High Risk Personnel Security. ..... 43
2.32. Associated Standards from DoD O-2000.12-H. ..... 43

**Attachment 1— GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 44**

**Attachment 2— REFERENCES TO DoD O-2000.12-H 53**

**Attachment 3— FORCE PROTECTION CONDITIONS (FPCONs) AND MEASURES 55**

**Attachment 4— TERRORIST THREAT LEVELS 59**

**Attachment 5— AOR-SPECIFIC TRAINING** 61

**Attachment 6— INFORMATION AND PROCEDURES FOR INSTALLATIONS RECEIVING AIR FORCE SECURITY FORCES CENTER AT/FP VULNERABILITY ASSESSMENTS** 63

**Attachment 7— LEVEL II AT/FP TRAINING SCHOOLS FOR AT OFFICERS/NCOS** 66

**Attachment 8—ANTITERRORISM RESOURCE ALLOCATION TEMPLATE** 68

# Chapter 1

## AIR FORCE AT PROGRAM

**1.1. Air Force AT 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, and counter terrorist incidents, allocating funds and personnel, and implementing AT measures.

**1.1.1. US Position on Terrorism.** The US position on terrorism is to encourage all nations to band together and give no sanctuary to terrorists. National security decision directives and statements by the President and senior officials set forth this policy. This instruction implements DoDI 2000.16, *DoD Antiterrorism Standards,* and adds Air Force-specific standards.

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

1.1.1.2. The US Government considers terrorism by any person or group to be a threat to US national security. It will resist the use of terrorism by any legal means. The US will take measures to protect its citizens, property, and interests when evidence exists that a state or any terrorist organization is mounting a terrorist act against this country.

1.1.1.3. The US Government will make no concessions to terrorists. Simultaneously, the US will use every available resource to gain the safe return of American citizens held hostage by terrorists.

1.1.1.4. The US will act decisively against terrorists without surrendering basic freedoms or endangering democratic principles. The US will encourage other governments to take similar stands.

**1.1.2. AT Responsibility.** AT is a command responsibility and must be thoroughly integrated into every unit mission. Commanders must continually review their AT posture to keep current with changing policies and threat levels. Risk management, based on current threat, is the key when determining vulnerabilities and resource prioritization. Any threat or potential vulnerability with risk that cannot be controlled to an acceptable level must be forwarded to the next level in the chain of command for resolution. AT also requires every individual's participation to maintain awareness, practice personal security measures and report suspicious activity.

**1.1.3. Countering the Threat.** Countering the terrorist threat requires a fully integrated and coordinated AT approach with a number of key areas that include at a minimum: Civil Engineers (readiness and security engineering), NBC Defense, EOD, Fire Protection, Services (food), Public Affairs, Communications, Intelligence, Operations, Security Forces, Surgeon General, Judge Advocate, Comptroller and Air Force Office of Special Investigations (AFOSI).

**1.1.4. 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, *DoD Antiterrorism Standards*, and DoD O-2000.12-H, *Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence*.

## Chapter 2

## DOD AND AIR FORCE ESTABLISHED STANDARDS

**2.1. DoD and Air Force Established Standards.** The following AT standards incorporate the DoD standards from DoDI 2000.16 and provide Air Force specific guidance. Air Force implementation of the DoD standards is contained in the subparagraphs following the DoD standards.

**2.1.1. DoD Standard 1 - DoD AT Policy.** Combatant Commanders, Chiefs of Service, and Directors of DoD Agencies and Field Activities (hereafter referred to collectively as "CINC and/or Services and/or DoD Agencies") are responsible for implementation of DoD AT policies within their organizations.

2.1.1.1. AF Deputy Chief of Staff, Air & Space Operations (AF/XO), is the OPR for Air Force AT matters and policy. AF/XO will approve all Air Force-wide AT programs.

2.1.1.1.1. The AF/XO chairs the FP Summit. The Force Protection (FP) Summit, serves as the primary organization to oversee Air Force efforts to improve and coordinate FP matters. Core members include MAJCOM/CVs, IL, JA, SC, SG, XP, DP, RE, SAF/IG, SAF/FM and the NGB/CF. Support members include XOF, XOI, SAF/IGX, HQ AFOSI, AFCESA, and the AF FP Battlelab. The FP Summit is chartered to:

2.1.1.1.1.1. Monitor the status of policy implementation.

2.1.1.1.1.2. Provide long term FP vision and direction.

2.1.1.1.1.3. Monitor the adequacy of AF-wide (MAJCOM) FP programs and resourcing methods to meet FP requirements in concert with the AF Corporate Structure.

2.1.1.1.2. The AF/XOF chairs the Air Staff FP Steering Group (FPSG). The FPSG is an Air Staff multidisciplined body chartered to meet semiannually to improve doctrine, policy, tactics, techniques and procedures for FP operations. The FPSG makes recommended policy changes to the AF/XO. Core members include: SAF/IGX, AF/ILE, AF/ILV, AF/SCX, AF/JAI, AF/SGX, AF/XOI, AF/XOO, AF/XPP, AF/REX, AF/FMB and ANG/DOF. As needed, additional FPSG core members include: AF/DPD, AF/ILT, AF/XOJ, AF/XON, AF/XOR and AF/XPM. Support members include: AFOSI Region Commanders, MAJCOM SF Directors, AF FP Battlelab, AFCESA, and AF Security Forces Center. The FPSG:

2.1.1.1.2.1. Provides advice to the AF FP Summit on short-and long-term measures to combat terrorism recommended by the AF Force Protection Working Group (AF FPWG).

2.1.1.1.2.2. Oversees the vulnerability assessment program.

2.1.1.1.2.3. Reviews medical support requirements for FP planning and force health protection.

2.1.1.1.2.4. Reviews policies affecting DoD travel security policy.

2.1.1.1.2.5. Reviews policies and guidelines for disseminating terrorist threat information.

2.1.1.1.2.6. Monitors nuclear, biological and chemical defense matters and policy.

2.1.1.1.2.7. Ensures AF installations develop AT programs according to this instruction.

2.1.1.1.2.8. Recommends/directs changes to existing programs and publications to enhance AF-wide FP operations.

2.1.1.1.2.9. Advises AF FP Summit on changes required to AF FP doctrine.

2.1.1.1.2.10. Reviews the adequacy of AT/FP training policy at all levels.

2.1.1.1.2.11. Reviews efforts to document and track AT/FP training.

2.1.1.1.2.12. Reviews integration into and the adequacy of FP training in PME and accession training.

2.1.1.1.2.13. Monitors FP requirements and works in concert with the Air Force Chief of Staff (CSAF) to balance the requirements with other mission essential needs.

2.1.1.1.2.14. Assesses the need for a standardized, service-wide template for identifying, prioritizing and costing AT/FP requirements.

2.1.1.1.2.15. Monitors efforts to maintain visibility of ANG and AFRC AT/FP requirements.

2.1.1.1.3. The Air Staff FP Working Group (FPWG), chaired by AF/XOFP, is an action officer level group meeting quarterly to work FP issues as directed by the FPSG. Core members are: IGX, ILEX, ILVR, SGXW, SCTI, JAI, XOFP, AFIAA, XOOO, and XOIA.

2.1.1.2. Air Force Director of Intelligence, Surveillance and Reconnaissance (AF/XOI):

2.1.1.2.1. Establishes polices and guidelines for gathering and disseminating foreign intelligence on international terrorism.

2.1.1.2.2. Provides all source analysis regarding capabilities, intentions, or activities of foreign governments or elements thereof, foreign organization, foreign persons and international terrorist activities of interest to the USAF.

2.1.1.2.3. Reviews requirements regarding proper levels of security clearances for leadership of deploying units and commensurate connectivity.

2.1.1.2.4. Represents USAF's foreign terrorism intelligence interests and equities to the national intelligence community.

2.1.1.2.5. Participates in national level indications and warning functions related to antiterrorism. The continuous interaction will occur primarily at the National Military Joint Intelligence Center (NMJIC) and in concert with the Joint Intelligence Task Force-Combating Terrorism (JITF-CT).

2.1.1.2.6. Ensures USAF and national intelligence collection operations and capabilities meet Air Force requirements.

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

2.1.1.3.1. Drafts and coordinates policy with the Air Staff FPSG and appropriate functional experts.

2.1.1.3.2. Develops guidance on AT and physical security enhancements.

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

2.1.1.3.4. Evaluates AT equipment and supplies.

2.1.1.3.5. Conducts antiterrorism vulnerability assessments of USAF/DoD sites as outlined in paragraph **2.26.**

2.1.1.3.6. Monitors worldwide terrorism incidents.

2.1.1.3.7. Addresses security and AT issues in operations plans and publications, where appropriate.

2.1.1.3.8. Relays to senior USAF leadership short and long-term measures to combat terrorism in coordination with AFOSI.

2.1.1.3.9. Provides support to AFOSI protective services.

2.1.1.3.10. Reports FP anomalies and suspicious incidents to AFOSI.

2.1.1.4. Air Force Surgeon General (AF/SG):

2.1.1.4.1. Serves as the office of primary responsibility (OPR) for total force health protection.

2.1.1.4.2. Ensures antiterrorism and force protection requirements are incorporated into Air Force Medical Service planning and programming.

2.1.1.4.3. Serves as member of the Force Protection Summit.

2.1.1.5. Assistant Surgeon for Medical Readiness, Science and Technology (SGX):

2.1.1.5.1. Attends the Force Protection Steering Group. Provides personnel to attend the FPWG.

2.1.1.5.2. Integrates medical readiness requirements into AT plans to include mass casualty planning, Weapons of Mass Destruction (WMD) identification and control, comprehensive health (disease/environmental/occupational) surveillance programs, food and water vulnerability assessments and other appropriate preventive medicine measures.

2.1.1.6. Air Force Medical Operations Agency (AFMOA). Develops medical operational guidance for mass casualty planning, WMD identification and command, comprehensive health (disease/environmental/occupational) surveillance programs, food and water vulnerability assessments and other appropriate preventive medicine measures.

2.1.1.7. Air Force Director of Transportation (AF/ILT):

2.1.1.7.1. Coordinates policies affecting DoD travel security policy and issues changes to all MAJCOMs and Field Operating Agencies (FOAs).

2.1.1.7.2. Distributes DoD Travel Advisories, and retransmits Office of the Assistant Secretary of Defense Special Operations/Low Intensity Conflict (OASD SO/LIC) messages regarding travel advisories.

2.1.1.7.3. Coordinates authorizations for non-tactical armored vehicles.

2.1.1.8. Air Force Director of Supply (AF/ILS):

2.1.1.8.1. Assists HQ AFOSI in programming for supply and equipment requirements necessary for implementing Air Force AT policy requirements.

2.1.1.8.2. Assists HQ AFOSI in programming for non-tactical armored vehicles.

2.1.1.9. Air Force Civil Engineer (AF/ILE):

2.1.1.9.1. Serves as the office of primary responsibility (OPR) for nuclear, biological, and chemical defense, explosive ordnance disposal (EOD), fire protection matters and policy.

2.1.1.9.2. Ensures civil engineers (CE) is included in all current and newly developed AT policies/issues.

2.1.1.9.3. Provides MAJCOMs with AT guidance on new and existing construction standards and furnishes a core member to the Air Staff FPSG.

2.1.1.10. Air Force Director of Services (AF/ILV):

2.1.1.10.1. Serves as the Air Force OPR for AT processes concerning food handling and distribution in coordination with the Defense Support Center Philadelphia.

2.1.1.10.2. Ensures Services is included in all current and newly-developed AT policies/issues.

2.1.1.10.3. Incorporates operational risk management and force protection measures into food handling procedures.

2.1.1.11. Secretary of the Air Force Public Affairs (SAF/PA):

2.1.1.11.1. Engages public affairs personnel to inform the public at the first indication of a terrorist incident.

2.1.1.12. Air Force Office of the Judge Advocate General (AF/JA):

2.1.1.12.1. Provides legal advice on AT through the International and Operations Law Division (AF/JAI).

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

2.1.1.13.1. Conducts counterintelligence activities, to include operations, investigations, collections, services, production, and analysis of threats from terrorism.

2.1.1.13.2. Maintains liaison and is the AF single point of contact with federal, state, local, and foreign nation law enforcement, counterintelligence and security agencies for terrorism and other matters falling within the AFOSI mission.

2.1.1.13.3. Provides warning of potential terrorist or unconventional warfare activities that are threats to Department of the Air Force personnel, property or assets worldwide.

2.1.1.13.4. Provides personal protective services for senior US, DoD, Air Force and allied officials.

2.1.1.13.5. Conducts countersurveillance activities or requests other agencies in support of the Air Force.

2.1.1.13.6. Manages the USAF Non-Tactical Armored Vehicle Program.

2.1.1.13.7. Assists in the provision of AT training.

2.1.1.14. MAJCOMs and installations shall establish FPWGs to serve as the commander's primary advisory body on AT policy and program management. Membership will include SF, MG,

DP, AFOSI, CE, SV, XP, OG, LG, SPTG, SC, IN, JA, FM, PA and representatives from all tenant units. Installation commanders may use the Installation Security Council (ISC) to fulfill this requirement.

2.1.1.15. Commanders at all echelons shall develop full working knowledge of AT policies and standards and take appropriate measures to protect DoD personnel to reduce the vulnerability of terrorist use of WMD.

**2.2. DoD Standard 2 - Development of AT Standards.** CINCs and/or Services and/or DoD Agencies shall develop and implement a comprehensive AT program under their respective control to comply with all the standards contained in DoDI 2000.16. CINCs and/or Services and/or DoD Agencies shall use standards contained in DoDI 2000.16 as baseline standards. CINCs and/or Services and/or Agencies may promulgate unique requirements in their implementing directives to supplement the standards contained herein.

2.2.1. As a minimum, AF standards shall address the areas listed in DoDI 2000.16 and this instruction to include:

2.2.1.1. Procedures to collect, analyze and disseminate terrorist threat information, threat capabilities and vulnerabilities to terrorist attacks. This is a joint responsibility of CINCs and/or Services and/or Agencies, and the intelligence community.

2.2.1.2. Terrorism Threat Assessment, Vulnerability Assessments, Terrorist Incident Response Measures and Terrorist Consequence Management Measures.

2.2.1.3. AT plans and procedures to enhance AT protection.

2.2.1.4. Procedures to identify AT requirements and program for resources necessary to meet security requirements.

2.2.1.4.1. AT Funding. There are two methods for obtaining AT funding. The first method is through the normal Program Objective Memorandum (POM) process. The Deputy Assistant Secretary of the Air Force (Budget) (SAF/FMB) includes approved AT budget requests in budget submissions and tracks program execution. SAF/FMB also provides policy and guidance on legal budget limitations and obligation criteria. Installations may use the template at attachment 8 for their POM submissions.

2.2.1.4.2. A second method of obtaining AT funding is through the Chairman of the Joint Chiefs of Staff (CJCS) Combating Terrorism Readiness Initiatives Fund (CbTRIF). Unlike POM submissions, CbTRIFs are to fund emergent high-priority combating terrorism requirements in the year of execution. CbTRIFs are not intended to replace the POM process or subsidize ongoing projects. They also do not supplement budget shortfalls or support routine activity that is normally a Service responsibility. Units may refer to Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5261.01, *Combating Terrorism Readiness Initiatives Fund* for specific guidance/fund submission process.

2.2.1.4.2.1. Air Force commands serving as components of combatant commands shall coordinate their requests IAW CbTRIF program guidelines. In addition, MAJCOMs shall provide a copy of their requests to SAF/FMBO and AF/XOFP, when they submit their request to the CINC. Once a submission is initially processed by the Joint Staff (J34), 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.

2.2.1.5. Construction considerations. All facilities shall comply with the DoD Antiterrorism Construction Standards.

**2.3. DoD Standard 3 - Assignment of AT Operational Responsibility.** When AT responsibilities for the CINCs and/or Services and/or DoD Agencies conflict or overlap, and are not otherwise governed by law, a specific DoD policy or an appropriate memorandum of agreement, the geographic CINC's force protection policies will take precedence over all force protection policies or programs of any DoD component deployed in that command's area of responsibility (AOR) and not otherwise under the security responsibility of the Department of State (DoS). Commanders at all levels shall take appropriate measures to protect DoD personnel, families, facilities, material and reduce the vulnerability to terrorist use of WMD.

2.3.1. MAJCOMs, Field Operating Agencies (FOAs), Direct Reporting Units (DRUs) and installation commanders shall identify AT specific operational responsibilities in their supplement to this instruction. Responsibilities shall include the scope of AT programs for facilities and operations that do not meet the legal definition of an installation (i.e., Recruiting Offices, Red Horse at Korea, ROTC and other Geographic Separated Units).

2.3.2. MAJCOMs, FOAs, DRUs and installation commanders shall ensure action to combat terrorism outside the United States comply with lead CINC, Service, or Agency guidance. MAJCOMs, FOAs, DRUs and installation commanders will also ensure such actions comply with applicable status of forces agreements (SOFA), the DoD Foreign Clearance Guide and MOUs.

2.3.3. MAJCOMs, FOAs, DRUs and installation commanders shall work with other Air Force organizations, US Service branches and DoD agencies to reduce vulnerability to terrorism. MAJCOMs FOAs, DRUs and installation commanders shall establish an AT program tailored to the local mission, conditions, the terrorist threat and the national security environment.

2.3.4. Installation commanders shall:

2.3.4.1. Implement an AT program to combat the local terrorist threat and support the US Air Force AT program. This program shall identify tasked agencies, required actions and means of exercising and evaluating the program through annual operational and command post AT exercises. Commanders will document a review of their Installation AT Plan on an annual basis or within 60 days of assuming command.

2.3.4.2. Establish an active public affairs program to combat terrorism. Public affairs personnel are the primary spokespersons for installation commanders. Public Affairs should help dispel rumors and misinformation by providing appropriate and timely information to the news media and base populace, according to current Office of Assistant Secretary of Defense for Public Affairs and SAF/PA AT guidance. Public Affairs Officers shall stay current on the subject of terrorism to enhance their effectiveness in dealing with this issue. Ensure all terrorist incidents/threat reports to news media are coordinated with installation commanders and his/her Threat Working Group prior to official release.

2.3.4.3. In coordination with AFOSI, provide assistance when directed or requested by the terrorist incident lead agency. The lead agency for terrorist incidents outside the United States is the

DoS. The Department of Justice (DoJ) is the lead agency for incidents within the United States. The Federal Aviation Administration (FAA) is the lead agency for certain aviation incidents.

2.3.4.4. Review, support, and implement DoD critical infrastructure protection requirements in accordance with DoD Directive 5160.54, Critical Infrastructure Protection (CIP) and AFPD 10-24, Air Force Critical Infrastructure Protection.

**2.4. DoD Standard 4 - AT Coordination in Overseas Locations.** CINCs and/or Services and/or DoD Agencies in overseas locations shall coordinate their AT efforts with host nation authorities and the US Embassy as appropriate. DoD Intelligence and Counterintelligence elements shall coordinate their activities in support of AT plans and programs through established DoD procedures.

2.4.1. CINCs with geographic responsibilities shall coordinate AT matters with Chiefs of Mission (CoMs) in countries within their AOR, and with functional CINCs and DoD Agencies, whose personnel are stationed in or transit the geographic CINC's AOR.

2.4.2. To ensure timely geographic CINC visibility of additional AT obligations, functional CINCs, and DoD Agencies, whose forces will station in or transit the AOR of a geographic CINC shall initiate coordination of AT matters with the geographic CINC.

2.4.3. DoD elements not under the force protection responsibility of a geographic CINC, by law or under provisions of a CINC-CoM MOA, shall comply with the State Department's Overseas Security Policy Board (OSPB) Security Standards.

2.4.4. The Director of the Defense Intelligence Agency (DIA), acting as DoD's executive agent for diplomatic security matters, shall, through the United States Defense Representative (USDR), ensure that non-CINC assigned DoD elements, whose AT responsibility rests with the CoM, comply with OSPB standards.

2.4.5. The Deputy Assistant Secretary of Defense (DASD) for Combating Terrorism Policy and Support (CTP&S), or designee, is DoD's designated representative for resolving disputes with DoS officials, in countries where the MOU on Security of DoD Elements and Personnel in Foreign Areas is between the DoS and the DoD. CINCs concerned with DoS standards shall address them with the DASD through the Chairman of the Joint Staff.

**2.5. DoD Standard 5 - Comprehensive AT Development, Implementation and Assessment.** Commanders at all levels shall develop and implement a comprehensive AT program for personnel under their respective control designed to accomplish all the standards contained in this Instruction.

2.5.1. AT Management. To develop and implement AT programs and plans, CINCs, Services, and/or DoD Agencies, shall designate a full-time staff officer in writing to supervise, inspect, exercise, review, assess and report on the AT program within the theater of command. At the theater level, component commanders provide the critical linkage from the CINC to the operating forces. Therefore, component commanders are responsible to provide direct AT/FP support to all forces, including transit forces. This direct support should include threat and VAs of routes and sites used by transiting forces, intelligence support, and AT augmentation. In order to effectively implement the standards in DoDI 2000.16, component commanders shall maintain a full-time Antiterrorism Officer (ATO) and consider a full-time AT/FP staff.

2.5.1.1. MAJCOM, FOA, DRU AT staff officers and installation ATOs shall be trained in AT procedures as described in DoDI 2000.16 and DoD O-2000.12-H. Training will include attendance at

a parent Level II Service-approved course (USAF approved courses are listed in **Attachment 7**). When possible, this training should be accomplished prior to assuming AT responsibilities.

2.5.2. Another critical link to operating forces is logistics support. The logistics contracting process for support of operational forces shall incorporate considerations for AT measures during contracting requirement, award, execution, and the evaluation process when the effort to be contracted for could affect the security of operating forces, particularly in-transit forces. Geographic CINCs shall ensure that component commanders, in coordination with the relevant country team, verify that all logistics support contracts and agreements consider AT for a particular security environment. During the evaluation process, future contract awards shall consider adequate AT performance.

2.5.3. Elements of the Comprehensive AT Program Development, Implementation and Assessment. AT program elements include threat assessments, VAs, planning, exercises, program reviews and training. The process, or sequence, of AT program elements should be iterative and serve to continuously refine the AT Plan.

2.5.4. AF Strategic Plan Performance Measures. Installations will report to MAJCOMs the status of their installation's AT plans IAW with AF Strategic Plan, Volume 2, Performance Measure 2.A.12, Antiterrorism/Force Protection Program. (RCS: HAF-SFC(SA)0125, Status of Antiterrorism Plans Report) This report is designated emergency status code C-2. Continue reporting during emergency conditions.

2.5.4.1. MAJCOMs will, in turn, report the status of their respective installations AT plan to HQ USAF/XOFP NLT 10 Oct and 10 Apr of each year. MAJCOMs will establish their own reporting suspenses for receiving installation information.

2.5.4.2. Further details regarding calculation data using this performance measure can be found at **https://www.afmia.randolph.af.mil/afmia/mip/mipp/perf_mgt/documents/vol2annex.doc**.

**2.6. DoD Standard 6 - Designation of Antiterrorism Officers (ATOs).** Antiterrorism Officers (ATOs) shall be assigned, in writing, at each installation or base, as well as deploying units (i.e., battalion, squadron, ship). Commanders shall designate a commissioned officer, non-commissioned officer or civilian staff officer, in writing as the ATO who shall be trained in AT procedures in a formal Service-approved Level II AT training course.

2.6.1. Installation commanders will designate, in writing, a commissioned officer, non-commissioned officer (E-6 or higher) or civilian equivalent as installation ATOs. Primary and alternates will be assigned. ATOs shall be trained in AT procedures in a formal service approved level II AT training course listed in **Attachment 7** and complete the training listed in Table 1.2.

2.6.2. Commanders deploying with their units outside the United States (US) and its territories and possessions, will assign a primary and alternate ATO as the unit's AT subject matter expert/advisor. The ATO shall ensure each person within the unit is aware of the terrorism threat, reporting procedures, and is trained to employ methods that reduce risk or mitigate the effects should an attack occur.

2.6.3. Commanders shall ensure ATOs have access to the AT publications listed in **Attachment 1**.

2.6.4. Installation ATOs shall:

2.6.4.1. In addition to regularly scheduled FPWGs, meets with installation AFOSI, Security Forces, Intelligence office, medical, fire, public health, and other agencies often enough to manage a comprehensive AT program. ATOs will at the same time work closely with intelligence per-

sonnel to ensure they possess the full spectrum of threat information. Installation ATOs shall review MOAs/MOUs with the functional experts, at a minimum annually, and assess the adequacy of the MOAs/MOUs to ensure installations are able to respond to terrorist threats/attacks.

2.6.4.2. Maintain liaison with MAJCOM AT staff officers to ensure AT currency.

2.6.4.3. Coordinate training allocations to ensure deploying units have a primary and alternate ATO assigned.

2.6.4.4. Organize installation FPWGs, analyze and track installation vulnerabilities and coordinate mitigation measures.

2.6.4.5. Work with installation exercise evaluation team chief and members, AFOSI, and base agencies to develop plausible exercise scenarios based on the threat (AFI 10-2501 is the source document for WMD exercises). Ensure the AT plan is exercised at least annually.

2.6.4.6. Assist commanders with preparing CbTRIF submission.

2.6.4.7. Organize and conduct installation VAs.

2.6.4.7.1. Assist commanders of deploying units in obtaining pre-deployment site VA reports and brief personnel on vulnerabilities and mitigation results.

2.6.4.8. Manage AT training efforts, to ensure all Unit Training Managers (UTMs) plan, receive and document required minimum training standards for Level I AT Awareness Training. Additionally, ensure AOR site-specific material is updated at least quarterly.

2.6.4.9. Review new construction with civil engineers from the early planning stage through project completion to ensure new and renovated projects meet minimum DoD Antiterrorism/Force Protection Construction Standards.

2.6.4.10. Serve as the OPR for the development of the installation's AT plan.

2.6.4.11. Monitors, tracks, and analyzes Random Antiterrorism Measures (RAMs) implementation efforts.

2.6.4.12. When designated by the installation commander, shall implement the responsibilities identified in AFPD 10-24, CIP to identify mission critical infrastructures and their vulnerability to terrorist attack.

**2.7. DoD Standard 7 - Application of Department of Defense (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.

2.7.1. 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 terrorism threat level terms are *Low, Moderate, Significant* and *High*, and are defined in **Attachment 4**. The system evaluates the threat using a variety of analytical threat factors. Defense Terrorism Warning Reports are used to convey terrorist groups are operationally active and specifically targeting US interests. Either DIA or the Combatant Commanders, regardless of a country's assigned threat level, issues warning reports.

2.7.2. The DIA sets the DoD general terrorism threat level identifying the potential risk to US personnel in a particular country. The DIA will coordinate, for clarity purposes, with DoS to minimize conflicting threat levels assigned by each organization. The DoD threat level applies whether or not US

personnel are present in the country. CINCs, with geographic responsibilities, may also set terrorism threat levels for specific personnel, family members, units and installations in countries within their AOR, using the definitions established by DIA. Commanders at all levels shall use their own threat analysis as the basis for developing plans and programs to protect assets for which they have AT responsibility. Terrorism Threat Levels are estimates with no direct relationship to specific Force Protection Conditions (FPCONs). A FPCON is a security posture promulgated by the commander in consideration of a variety of factors (i.e., a terrorist threat analysis, threat level, etc.). Threat levels should not be confused with FPCONs.

2.7.3. Effective application of the DoD 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 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 a variety of intelligence information about a specified terrorist group to determine an individual, unit, facility and/or an installation's vulnerability to a specific form of terrorist attack based on capabilities of terrorists and terrorist groups. Thus, the threat analysis should be supported by intelligence gathering (overseas) and information gathering (domestically) on the part of appropriate authorities.

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

2.8.1. To support the commander, the Services should continuously ensure that forces are trained to maximize the use of information derived from law enforcement liaison, intelligence, and counterintelligence processes and procedures. This includes intelligence procedures for handling priority intelligence requests for in-transit units, as well as, implementation of procedures to conduct intelligence preparation of the battlefield and mission analysis.

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

2.8.3. A terrorism 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, can and should encourage personnel under their command to report information on individuals, events or situations that could pose a threat to the security of DoD personnel, families, facilities and resources.

2.8.4. At a strategic level, 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.

2.8.5. Headquarters Air Force Office of Special Investigation (HQ AFOSI) has primary responsibility for the collection, all source tactical analysis, production and dissemination to U. S. military com-

manders, the DOD and U.S. Intelligence communities of terrorist threat information gathered from federal, state and local authorities, host nation security services, and counterintelligence (CI) sources.

**2.9. DoD Standard 9 - Threat Information Flow.** Commanders, at all levels shall forward up and down the chain of command all information pertaining to suspected terrorist threats or acts of terrorism involving DoD personnel or assets for which they have AT responsibility.

2.9.1. The pattern of terrorist surveillance, targeting and planning is best recognized through the sharing of information. These efforts shall include the chain of command and the interagency process, at the appropriate level. When local information indicates gaps, unit commanders should forward timely requests for information to AFOSI, AF Intelligence, or other organizations via appropriate intelligence collection and production channels. Likewise, Component Commanders shall provide transiting units with tailored terrorist threat information.

2.9.2. Installation commanders shall establish a Threat Working Group (TWG) to address the threat. TWGs generally consist of personnel from AFOSI, IN, SF, SG (Medical Intelligence Officer) and the installation ATO. A TWG's primary function is to assess the threat for the commander and recommend courses of action to mitigate or counter the threat. Installation commanders should consider adding other agencies, particularly CE and SV, as appropriate, to enhance the TWG. A TWG does not fulfill the function of a FPWG. The TWG will meet, at a minimum, weekly to review the current threat and advise the installation commander accordingly.

2.9.3. The installation's/activity's servicing AFOSI detachment is the primary focal point for collecting and reporting the terrorist threat. AFOSI detachments obtain terrorist threat information from a wide variety of counterintelligence activities and other sources of information.

2.9.4. Commanders, down to the installation level, shall develop procedures to ensure Terrorism Threat Advisories, Terrorism Warning Reports, Terrorism Threat Level changes, and FPCON changes are immediately disseminated to all personnel and, as appropriate, supporting law enforcement agencies. Commanders should consider using "Giant Voice," commander access cable channels, cable overrides, e-mail, marquees and any other methods that rapidly disseminate threat information to all personnel.

**2.10. DoD Standard 10 – Potential Threat of Terrorist Use of Weapons of Mass Destruction (WMD).** Commanders, at all levels shall take appropriate measures to protect DoD personnel, families, facilities and material, and reduce the vulnerability to terrorist use of WMD. Thus, CINCs and/or Services and/or DoD Agencies shall develop WMD Threat Assessments for potential terrorist use of WMD against personnel and assets for which they have AT responsibility. Reports through the chain of command shall be processed immediately when significant information is obtained identifying organizations with WMD capabilities.

2.10.1. 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.

2.10.2. HQ AFOSI will incorporate terrorist use of WMD into their installation's threat assessment.

**2.11. DoD Standard 11 - Adjustment of Force Protection Conditions (FPCONs).** Combatant commanders have ultimate AT and force protection authority and responsibility within their AOR. Service chiefs are responsible for AT and force protection authority for those personnel and assets for which they

have AT responsibility within the 50 United States. Commanders at all levels shall develop a process, based on terrorism threat information and/or guidance from higher headquarters, to raise or lower FPCONs.

2.11.1. The process to raise or lower FPCONs shall be tailored to the local mission and allow higher headquarters to direct downward implementation. The FPCON process shall comply with the guidance contained in DoD O-2000.12-H.

2.11.2. Downward directed FPCONs (force protection condition alerting message [FPCAM]) require implementation of all measures for that FPCON, as listed in DoD O-2000.12-H, unless the directing authority grants relief.

2.11.2.1. Periodically, after the initial FPCON implementation date, installation commanders shall reassess the local threat and report to higher headquarters conditions that would warrant a change to the current FPCONs and proposed measures to be taken based on the reassessment

**2.12. DoD Standard 12 - FPCON Measures Implementation.** CINCs and/or Services, and/or DoD Agencies shall ensure that FPCON transition procedures and measures are properly implemented and disseminated by subordinate commanders.

2.12.1. Tenant units, regardless of MAJCOM or service component, shall conform to the host installation's FPCON. Additionally, tenants shall participate in all exercises with the host unit.

2.12.2. All agencies shall report their FPCON changes IAW AFMAN 10-206, *Operational Reporting*. MAJCOM/SFs and FOAs will relay the FPCON change as soon as possible to HQ AFSFC Operations Center, DSN: 473-0960, or **mailto:SIPRNET** **hqafsfc@acc.af.smil.mil** and/or STU III DSN: 473-5543 for secure communications.

**2.13. DoD Standard 13 - FPCON Measures.** Commanders at all levels, both stationary and in transit, shall develop site-specific measures or action tasks for each FPCON which supplements those measures/actions enumerated for each FPCON as listed within Appendix A of DoD O-2000.12-H (reference c). An AT Plan with a complete listing of site-specific AT measures, linked to a FPCON, will be classified, as a minimum, CONFIDENTIAL. When separated from the AT Plan, site-specific AT measures and FPCONs remain FOR OFFICIAL USE ONLY (if classification is necessary, mark as follows: Classified by: DoDI 2000.16, Standard 13, 14 Jun 01; Reason: 1.5(a); Declassify on: X4). These measures will change as the threat situation increases from FPCON Normal to FPCON Delta.

2.13.1. In developing site-specific FPCON measures, the commander must always consider those additional FPCON measures, which permit sufficient time and space to determine hostile intent, particularly in accordance with the Standing Rules of Engagement. The component commander's organic intelligence, counterintelligence, law enforcement resources, institutional knowledge of their area of AT responsibility and comprehensive understanding of unit capabilities, supported by national and theater assets, shall be leveraged in directing tailored FPCON measures to be implemented at specific sites for both stationary and in-transit units. To support both the component and local commanders in this effort, CINCs with geographic responsibilities should negotiate with host nations for authority to implement AT measure to provide such time and space.

2.13.2. Commanders, at all levels (i.e. installation, tenant, GSU levels etc), shall establish local measures to supplement DoD O-2000.12-H procedures to transition between FPCONs. Whereas Terror-

ism Threat Levels are analytical assessments of terrorist activity in a country, FPCONs are graduated categories of measures or actions commanders take to protect personnel and assets from attack.

2.13.2.1. Commanders, at all levels shall set local FPCONs. Subordinate commanders may raise a higher-level commander's FPCON for those personnel and assets for which they have AT responsibilities. However, subordinate commanders shall not lower a higher commander's FPCONs without the higher-level commander's concurrence. Commanders shall ensure proper notifications are made.

2.13.2.2. Installation and GSU commanders shall establish specific FPCON measures (tailored to the local mission, conditions, and the terrorist threat) to augment the DoD FPCON measures, listed in **Attachment 3**.

2.13.2.3. Installation commanders must continuously evaluate available information about local terrorist activity to determine whether a terrorist threat to installation facilities or personnel exists. If the information warrants action, select and declare the appropriate FPCON. Commanders may modify their locally developed FPCON measures based on their requirements and to counter local threats.

2.13.3. Installation commanders, in coordination with the installation TWG and/or FPWG, shall review local FPCON measures semi-annually to ensure threat mitigation measures are appropriate. Consideration shall be given to the most recent VA and current AFOSI counterintelligence threat assessment, when conducting this review.

2.13.4. Installation and GSU commanders shall develop and implement a Random Antiterrorism Measures (RAM) program according to DoD O-2000.12-H that will include all units on the installation. The RAM program shall be included in AT plans and tie directly with all FPCONs (including FPCON Normal), as listed in DoD O-2000.12-H to ensure continuity and standardization among the Services, should threats require USAF-wide implementation. Installations shall add local measures as required.

2.13.4.1. At least three RAMs chosen from higher FPCONs are required daily. RAM times for implementation, location and duration shall be regularly changed to avoid predictability.

2.13.4.2. RAM execution shall be broad based and involve all units and personnel. ATOs are required to monitor, track and analyze RAM implementation efforts. Installation commanders will develop procedures to ensure RAMs are being conducted and reported to the ATO.

2.13.5. Installation commanders shall incorporate AT measures in plans for functions such as change of commands, open houses, air shows and organized off-base activities.

**2.14. DoD Standard 14 - Commanders Shall Maintain a Comprehensive AT Program for Those Personnel and Assets for Which They Have AT Responsibilities.** Planning is critical to deterrence, detection, defense and response to terrorist incidents. Where possible, commanders may use as a guide, the DoD Deputy Directorate for Operations (Combating Terrorism) J34, AT/FP Planning Template CD-ROM and WMD Appendix. in DoDI 2000.16. The AT plan and elements shall clearly describe site-specific AT measures. The AT plan and elements should be written from the CINC, Service, or DoD Agency level, down to the installation level for permanent operations or locations and incorporated in operations orders for temporary operations or exercises.

2.14.1. To be proactive, all AT programs shall include tenets of countersurveillance (CS), counterintelligence (CI) and other specialized skills as a matter of routine, and shall identify an appropriate organization as the focal point for the integration of local and/or host nation intelligence, counterintelligence and criminal intelligence information into AT operations. To that end, commanders at all levels shall constantly strive to ensure that proactive techniques and assets can be incorporated to detect and deter terrorists. CINCs and Services should ensure component commanders incorporate CI/CS assets in support of in-transit units, particularly at higher threat-level areas.

2.14.2. Commanders, down to installation and GSU level, will develop and implement an AT plan. Commanders may use a stand-alone plan or include AT annexes in their existing force protection plan. Guidelines on AT planning are found in AFMAN 10-401, Volumes 1 & 2. Stand-alone documents (i.e., Standard Operating Procedures, local regulations, or Operations Orders that articulate requirements for AT key elements) shall be replicated in and/or referenced in the AT Plan. Task appropriate level units for support, ensuring all organic, tenant and supported units are considered, and receive copies of the plans.

2.14.3. At a minimum, the AT Plan shall address the following key elements:

2.14.3.1. Terrorism Threat Assessment (see Standard 15)

2.14.3.2. Vulnerability Assessment (see Standard 26)

2.14.3.3. Risk Assessment (see Standard 15)

2.14.3.4. AT Physical Security Measures (see Standard 16)

2.14.3.5. Terrorist Incident Response Measures (see Standard 17)

2.14.3.6. Terrorist Consequence Management Measures (see Standard 18)

**2.15. DoD Standard 15 - Terrorism Threat Assessment.** Commanders shall prepare a terrorism threat assessment for those personnel, assets, and mission critical infrastructures for which they have AT responsibilities. Threat assessments shall be prepared at least annually and should identify the full range of known or estimated terrorist capabilities for use in conducting VAs and planning countermeasures. Threat analysis is required to adequately support risk management decisions of both stationed forces within, and those in-transit through, higher-threat areas including ports, airfields and inland movement routes. Terrorism threat assessments shall be the basis and justification for recommendations on AT enhancements, program/budget requests and the establishment of FPCONs.

2.15.1. The terrorism threat assessment is the tool that commanders shall use to arrive at a judgment of risk and consequences of terrorist attack. Commanders shall integrate threat information prepared by the intelligence community, technical information from security and engineering planners and information from other sources to prepare their assessments. In addition to the annual threat assessment used for AT Program planning, continuous analysis of threat information is required to support the threat warning process.

2.15.2. CINCs and/or Services, and/or DoD Agencies shall designate which subordinate commanders will prepare these terrorism threat assessments. This normally applies to installation commanders and above.

2.15.2.1. AFOSI will provide the installation's counterintelligence threat assessment, which will address the threats from terrorism, agitational and subversive groups, criminal elements, and for-

eign intelligence services. The counterintelligence threat assessment will be prepared annually and as changes in the threat require. AFOSI shall also provide a counterintelligence threat assessment to Air Force units deploying overseas. Upon notification of deployment, unit commanders will immediately contact their servicing AFOSI detachment and request a counterintelligence threat assessment. The assessment will be provided within 15 days of the unit's departure. .

2.15.3. The process of producing terrorism threat assessments should include, as a minimum, liaison with the country team, host national security, husbanding contractor, and port authority, where applicable.

2.15.4. Risk assessments provide commanders with a method to assist them in making resource allocation decisions designed to protect their people and assets from possible terrorist threats in a resource-constrained environment. Commanders shall conduct risk assessments to integrate threat and vulnerability information in order to make conscious and informed decisions to commit resources or enact policies and procedures to mitigate the threat or define the risk. A risk assessment allows the commander to obtain a clear picture of the current AT posture and identify those areas requiring improvement. During the risk assessment, important information is collected to assist in writing the overall AT Plan. While conducting risk assessments, commanders shall consider the following four elements:

2.15.4.1. The terrorist threat.

2.15.4.2. The criticality of infrastructures, facilities and assets.

2.15.4.3. The vulnerability of critical infrastructures, facilities, food and water, programs, and systems to acts of terrorism (refer to paragraph **2.26.**).

2.15.4.4. The ability to conduct activities to deter terrorist incidents, employ countermeasures, mitigate the effects of a terrorist incident, and recover from a terrorist incident.

2.15.5. The installation risk assessment must be reviewed annually by the Installation FPWG.

**2.16. DoD Standard 16 - AT Physical Security Measures.** AT physical security measures shall be considered, must support, and must be referenced within the AT Plan to ensure an integrated approach to terrorist threats. Where there are multiple commanders at an installation, the installation commander is responsible for coordinating and integrating individual unit physical security plans and measures into the AT Plan.

2.16.1. Tenant and in-transit units will comply with the host installation's AT physical security measures.

2.16.2. The AT physical security measures shall integrate facilities, equipment, trained personnel and procedures into a comprehensive effort designed to provide maximum AT protection to personnel and assets. Well-designed AT physical security measures include detection, assessment, delay, denial and notification. This is best accomplished through the development of a synchronized matrix that outlines who will do what, where, when and how. The measures should include provisions for the use of physical structures: physical security equipment; chemical, biological, radiological detections and protection equipment; security procedures; RAMs; response forces and emergency measures sufficient to achieve the desired level of AT protection and preparedness to respond to a terrorist attack. RAMs constitute a particularly effective method of deterrence of terrorist attack and should be used for both in place and transiting forces.

2.16.2.1. Installation commanders shall incorporate physical security actions for the installation's AT program in the installation security plans, full spectrum threat response plan, public affairs plans and/or resource protection plans. Forward all plans to the installation ATO. Plan actions shall be incorporated into the overarching AT plan and include the following:

2.16.2.1.1. AT physical security measures.

2.16.2.1.2. FPCON measures (must be site specific).

2.16.2.1.3. Access control and entry control points.

2.16.2.1.4. Mass notification.

2.16.2.1.5. Delay elements - barrier plan, perimeter controls, RAMs and sensors.

2.16.2.1.6. Response elements - security and law enforcement assets, contract/hired forces, unit guards, Resource Augmentation Duty (READY) and on-call support from reaction forces.

2.16.2.1.7. Assessment of appropriate response measures, installation priorities and procedures for enhanced AT measures.

2.16.2.1.8. Vulnerabilities and associated countermeasures (i.e., measures in a classified annex).

2.16.2.1.9. AT training and education.

2.16.2.1.10. Physical security of family members.

2.16.2.1.11. Coordination/integration of individual unit physical security plans and measures.

2.16.3. The installation barrier plan shall list in priority order: gates, roads and facilities to be protected and types of passive barriers (i.e., serpentine jersey barriers, speed bumps, hedgehog barriers) to be used. The plan will detail the number of barriers required, where the barriers will be maintained/pre-positioned, the required equipment and the personnel assigned to move them and a detailed map of where/how the barriers will be placed. Installation commanders are highly encouraged to pre-position barriers at installation gates and key facilities to allow for the most rapid response to increased threats. Include basic elements of this plan as sub-elements of installation FPCON measures.

**2.17. DoD Standard 17 - Terrorist Incident Response Measures.** Limiting the effects and the number of casualties resulting from an attack will undermine the terrorist's overall objectives. An effective incident response strategy and capability can contribute to deterring terrorist attacks if our adversaries recognize the US ability to limit the effects of their attacks. Thus, installation and/or afloat commanders shall prepare installation-wide and/or shipboard terrorist incident response measures. These measures shall include procedures for determining the nature and scope of terrorist incident response; procedures for coordinating security, fire and medical first responders; and steps to reconstitute the installation's ability to perform AT measures. Terrorist Incident Response measures should address the full scope of an installation's response to a terrorist 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.

2.17.1. Terrorist incident response measures shall include emergency response and disaster planning/consequence management for installation engineering, security, law enforcement, 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.

2.17.1.1. It is critical that geographic CINCs are able to deploy in a timely manner an organic Terrorist Incident Response Team capable of providing advice to the host nation, supporting emergency lifesaving and rescue functions, providing protection to DoD personnel and property, reducing the effects of further damage, and when appropriate, conducting/supporting criminal investigations. This preparation shall include the integration of teams in contingency planning for in-transit units. All MAJCOMs shall prepare command-wide terrorist incident response measures and ensure integration with the appropriate geographic CINC's Terrorist Incident Response Team.

2.17.1.2. Terrorist incident response measures shall include host nation/local law enforcement procedures to coordinate and employ response including communications, security, fire, explosive ordnance disposal (EOD) and medical. As terrorist attacks are criminal acts subject to prosecution, preservation of the scene for evidence collection and processing shall be addressed to the extent possible and when it would not jeopardize human life.

2.17.2. Installation commanders shall establish an incident response plan to ensure the installation can respond to a terrorist attack. This plan may be 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 measures, handle mass casualties and other areas as outlined in DoD Standard #17. For more detailed response measures to incidents involving WMD, refer to Annex D to the Full Spectrum Threat Response Plan, OPLAN 10-2., which may be cross-referenced as a sup-portion of the overall installation AT plan. This plan will, as a minimum, be exercised annually.

2.17.3. Installation service contracts will include measures to preclude the unmonitored presence of cleaning or other service personnel in vulnerable facilities. Contracts should also include procedures to have personnel consent to criminal background checks prior to being granted entry onto the installation.

2.17.4. Installation entry control procedures will be established for non-base connected personnel attending education classes, sporting events teams or other functions. Individuals should be briefed that their privileges are restricted to transit to and from the location of the activity. Installations should consider a means to readily identify (by distinctive pass or other identification) vehicles and personnel admitted to the installation for these purposes.

2.17.5. Inclusion of Off-Installation Personnel in AT Plans. Commanders shall ensure Terrorism Incident Response measures contain current residential location information for all DoD personnel and their family members, when stationed outside of the United States, territories, and possessions in Moderate, Significant and High Terrorism Threat Level areas. Such measures should provide for enhanced security and/or possible evacuation of DoD personnel and their dependents. Furthermore, commanders in Moderate, Significant and High Terrorism Threat Level areas should investigate special security arrangements to protect DoD personnel and their dependents living on the economy. Close coordination with other US government agencies and the host nation is essential to ensure effective allocation of security resources and protection of DoD personnel.

**2.18. DoD Standard 18 - Terrorist Consequence Management Measures.** Although not an element of AT, commanders shall include terrorist consequence management preparedness and response measures as an adjunct to the installation AT Plan. The Terrorist Consequence Management measures should include emergency response and disaster planning and/or preparedness to respond to a terrorist attack for installation engineering, logistics, medical, mass casualty response, transportation, personnel administration and local and/or 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. Terrorist use of WMD, or terrorist attacks on dignitaries, while visiting DoD installations, will require immediate close coordination with higher command and the host nation and/or federal, state, and local authorities.

2.18.1. Terrorist Consequence Management planning will be in accordance with AFI 10-2501 and will address:

2.18.1.1. Response assessments to terrorist use of WMD and identification of long-term upgrade requirements and appropriate measures to mitigate potential threats.

2.18.1.2. Recovery plans/annexes specifically addressing command, control and communications between local, state and host nation emergency assistance agencies, procedures to protect, respond to and reduce the vulnerability of USAF personnel to WMD. Installation plans shall clearly identify first responders and other follow-on support teams.

2.18.1.3. Appropriate measures, including attack warning, to notify and protect personnel and reduce the vulnerability to the threat of use of WMD. Plans shall identify responders, specific local/host nation support, ensure appropriate antibiotics and antidotes are supplied, personnel are trained and that all personnel (including family members) are aware of the threat and can respond accordingly.

2.18.1.4. Mass casualty response includes: casualty triage procedures, (medical treatment, decontamination, evacuation and tracking, site security, evidence preservation and contamination control measures and detailed interagency support and coordination measures.

2.18.1.5. Ensure first responders and treatment personnel are designated, trained, and equipped to respond to WMD/HAZMAT incidents IAW AFPD 10-26, *Counter-NBC Operational Preparedness;* AFI 10-2501, *Full Spectrum Threat Response, Planning and Operations;* AFH 20-2502, *USAF Weapons of Mass Destruction Threat Planning and Response Handbook;* AFI 32-4002, *HAZMAT Planning and Response Operations* and AFI 41-106*, Medical Readiness Planning and Training.*

**2.19. DoD Standard 19 - Training and Exercises.** Commanders, (ship, squadron, battalion-level and above), shall conduct field and staff training to exercise AT Plans, to include AT physical security measures, terrorist incident response measures, and terrorist consequence management measures, at least annually. AT training and exercises shall be provided the same emphasis afforded combat task training and executed with the intent to identify shortfalls impacting the protection of personnel and assets against terrorist assault and subsequent consequence management efforts. AT training, particularly pre-deployment training, shall be supported by measurable standards and include credible deterrence/response, tactics, techniques, and procedures. AT training shall also be incorporated into unit-level training plans and pre-deployment exercises. To realize incorporation of lessons learned, commanders should maintain exercise documentation for no less than one year.

2.19.1. Commanders, at all levels, shall ensure joint and/or combined operations and/or exercises incorporate AT training and planning for forces involved. To realize incorporation of lessons learned:

2.19.1.1. AF installations/sites shall exercise and evaluate the installations overall AT Awareness posture IAW Table 1.1 of this instruction and DoDI 2000.16, Standard 22, table 1.1. Exercise the installation terrorism incident response plan annually.

2.19.1.2. Pre-deployment training regimes shall include credible deterrence and response standards and deterrence-specific tactics, techniques and procedures. Pre-deployment training shall also include terrorist scenarios and hostile intent decision-making.

2.19.1.3. AT training shall also be incorporated into unit-level training plans and exercises.

2.19.1.4. Installation commanders will ensure base-wide training exercises are conducted annually IAW the AT Plan. The exercises shall include all FPCON measures, evacuation procedures, notification plan, terrorist use of WMD and other key areas outlined in their installation's AT Plans.

**2.20. DoD Standard 20 - Comprehensive AT Review.** Commanders at all levels shall review their own AT Programs and Plans at least annually to facilitate AT program enhancement. Furthermore, for the same purpose, commanders at all levels shall likewise review the AT program and plan of their immediate subordinate in the chain of command at least annually. While such reviews do not constitute a VA, they are intended to ensure compliance with the standards contained in this Instruction. To ensure the design and implementation of physical security measures coincident with the AT program are consistent with the local terrorist threat level, AT programs shall also be reviewed when the terrorism threat level changes.

2.20.1. AF installations/sites will review and exercise their AT Program/Plan, listed in paragraph **2.20.**, at least annually.

**2.21. DoD Standard 21 - General Requirements for AT Training.** CINCs and/or Services and/or DoD Agencies shall ensure all assigned personnel receive appropriate training to advance AT awareness. Individual records shall be updated to reflect AT training in accordance with DoD Component policy.

2.21.1. AF installations/sites will update AT awareness training IAW AFI 36-2201, *Air Force Training Program.*

**2.22. DoD Standard 22 - Level I AT Awareness Training.** CINCs and/or Services and/or DoD Agencies shall ensure that every military service member, DoD employee, and local national hired by the DoD, regardless of rank, is made aware of the need to maintain vigilance for possible terrorist actions and employ AT tactics, techniques and procedures, as discussed in DoD O-2000.12-H and Joint Pub 3-07.2. Furthermore, the Air Force shall offer Level I AT Awareness Training to contractor employees, under terms and conditions as specified in the contract.

2.22.1. CINCs, and/or Services, and/or DoD Agencies shall ensure every family member accompanying DoD personnel overseas is made aware of the need to maintain vigilance for possible terrorist actions and employ AT tactics, techniques and procedures, as discussed in 2000.12H and Joint Pub 3-07.2. Thus, family members 14 years and older (or younger at discretion of the DoD sponsor) traveling beyond CONUS on official business, (i.e. on an accompanied permanent change of station move) shall receive Level I AT Awareness Training as part of their pre-departure requirements. Fur-

thermore, the commander should encourage family members to receive Level I AT Awareness Training prior to any OCONUS travel ( i.e., leave).

2.22.2. Individual security awareness and individual AT training are essential elements of an overall AT program. Each individual must be exposed at the earliest opportunity to share the responsibility of ensuring alertness and the application of personal protection measures. Therefore, CINCS/and/or Services and/or DoD agencies shall provide Level I AT Awareness Training in basic training or in general military subject training for all initial entry Service and DoD Agency personnel.

2.22.3. Thereafter, CINCs, and/or Services, and/or DoD agencies shall provide Level I AT Awareness Training:

2.22.3.1. Annually to all OCONUS-based DoD personnel.

2.22.3.2. Annually to all CONUS-based DoD personnel who are eligible for OCONUS deployment. Active uniformed CONUS-based members of the CINCS and Services shall receive Level I training annually. Subsequently, DoD personnel deploying OCONUS shall be provided, within 3 months of deployment, an AOR update (refer to DoD Standard 23 below).

2.22.3.3. Annually to all CONUS-based DoD personnel, regardless of duty status, if the CONUS Terrorism Threat Level is promulgated above "MODERATE."

2.22.3.4. Annual Level 1 AT awareness training may be accomplished by any level II certified personnel or per DoD sponsored computer-based training and/or distance learning.

2.22.4. Level I training shall be documented as follows:

2.22.4.1. The Military Personnel Flight (MPF) Outbound Assignments Section will document Level I training for individuals, and their dependents that are 14 years or older, relocating due to an OCONUS PCS on the relocation checklist. The checklist will include this training requirement in their relocation-processing letter. Training must be completed prior to final out-processing.

2.22.4.2. Unit Deployment Managers (UDMs) shall document Level I training for individuals projected for TDY OCONUS. UDMs will ensure individuals receive the training prior to deployment. Additionally, unit ancillary training managers will document Level I AT Awareness Training with the date of completion in Military Modernization Personnel Data System (MILPDS).

2.22.4.3. Unit training mangers shall document Level 1 AT awareness training through normal ancillary records when documentation through PCS/TDY checklist or MILPDS is not possible.

2.22.5. The unit responsible for preparing orders shall refer to DoD 4500.54-G, *DoD Foreign Clearance Guide* (can be web-accessed at **http://www.fcg.pentagon.mil/fcg/geninfo1.htm**) for individuals going PCS or TDY and ensure compliance and documentation of AT training.

2.22.6. AF installation/site commanders shall:

2.22.6.1. Develop procedures to ensure Level I AT Awareness Training is offered to all military service and DoD employee family members traveling OCONUS on unofficial travel such as leave.

2.22.6.2. Ensure everyone traveling to DoD-designated high physical threat countries, as defined in the Foreign Clearance Guide, receives (briefed) the OASD SO/LIC or USAF/ILT DoD Travel Security Advisories and any Federal Aviation Administration (FAA) travel advisories.

2.22.6.3. Report quarterly to HQ USAF/XOFP, (through installation ATOs through MAJCOM ATOs) all personnel who arrive on-station without Level I AT Awareness Training. Full Name,

Rank, Sending Unit, Sending MAJCOM, Receiving Unit, Receiving MAJCOM and total number of gains for the period shall be included in the report. (RCS: HAF-SFC(AR)0126, Training Reports for Antiterrorism Level I and Level II Training) This report is designated emergency status code C-2. Continue reporting during emergency conditions.

2.22.7. USAF Strategic Plan Performance Measures. Installations will report to MAJCOMs the status of their installations Level I training status IAW with Air Force Strategic Plan, Volume 2, Performance Measure 2.A.14, Implementation and Tracking of Level I Antiterrorism Training. (RCS: HAF-SFC(AR)0126, Training Reports for Antiterrorism Level I and Level II Training) This report is designated emergency status code C-2. Continue reporting during emergency conditions.

2.22.7.1. MAJCOMs will, in turn, report the status of their respective installations to HQ USAF/XOFP NLT 15 Oct and 15 Apr of each year. MAJCOMs will establish their own reporting suspenses for receiving installation information.

2.22.7.2. Further details regarding this Performance Measure can be found at **https://www.afmia.randolph.af.mil/afmia/mip/mipp/perf_mgt/documents/vol2annex.doc**.

2.22.8. Individuals may become qualified to administer Level I AT Awareness Training via two methods:

2.22.8.1. Attending a formal Service-approved Level II ATO Training course of instruction (see Table 1.2 for minimum training standards). The training must include a review of current AT publications and methods for obtaining AOR-specific terrorism threat analysis, updates and warnings.

2.22.8.2. Certification by the installation commander. Installation commanders, may qualify individuals who are subject matter experts and have received formal training in AT and individual protection measures (i.e., security forces, AFOSI special agents, etc.) and who have received specific formal training in AT tactics, techniques, and procedures. Installation commanders may individually exempt these individuals from the Level II ATO training requirements, as outlined in Table 1.2, if the individuals have also received training that covers reviewing current AT publications and identifying methods for obtaining AOR-specific updates.

2.22.8.2.1. All Air Force AT Officers/NCOs (required by Standard 6) will receive formal education at an approved Level II course. This requirement cannot be waived. Installation commanders may qualify individuals to deliver Level I training, as stated in the previous paragraph, but not designate them as their Standard 6 AT Officer/NCO. **Attachment 7** lists USAF approved courses.

2.22.9. HQ AFOSI and HQ AFSFC/SFP jointly develop AT awareness briefings for use in delivering Level I training. AFOSI will prepare and ensure the AOR specific terrorist threat is updated quarterly or when significant changes in the threat warrant. Level I training offered by other Services or DoD agencies meets DoD requirements as long as they fulfill all requirements listed in Table 1.1.

2.22.9.1. **Table 2.1.** below outlines Level I AT Awareness Training requirements.

**Table 2.1. Level I AT Awareness Training.**

| Level of Training | Target Audience | Minimum Training Standard |
|---|---|---|
| Level I<br>AT<br>Awareness Training<br>Provided annually to:<br>(1) All OCONUS-based DoD personnel.<br>(2) All active uniformed CONUS-based members of the CINCs and Services.<br>(3) All CONUS-based DoD personnel eligible for official OCONUS travel on government orders.<br>(4) All CONUS-based DoD personnel regardless of duty status, if the CONUS Terrorism Threat Level is promulgated above "MODERATE."<br><br>Graduates will have requisite knowledge to remain vigilant for possible terrorist actions and employ AT tactics, techniques, and procedures, as discussed in DoD O-2000.12-H and Joint Pub 3-07.2. | DoD personnel accessions during initial training<br><br>Military, DoD civilians, their family members 14 years old and greater (when family members are deploying or traveling on government orders) and DoD-employed contractors. | Service-provided instruction; incorporates Service-standardized Principle of Instruction (POI) consisting of the following minimum topics:<br>1. Viewing the Service-selected personal awareness video provided under the instruction of a qualified Level I AT Awareness instructor and/or DoD-sponsored computer-based and/or distance learning (DoD personnel accessions must receive initial training under instruction of a qualified Level I AT Awareness Instructor).<br>2. Instruction on the following: *Introduction to Terrorism Terrorist Operations Individual Protective Measures Terrorist Surveillance Techniques Improvised Explosive Device (IED) Attacks (**NOTE:** Ensure special emphasis is placed on secondary IED tactic.) Kidnapping & Hostage Survival Explanation of Terrorism Threat Levels and FPCON System*<br>3. 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.)<br>4. Receipt of AOR updates three months prior to travel to include current threat brief and AOR- specific requirements, as provided by the receiving geographic CINC. |

**2.23. DoD Standard 23 - AOR-Specific Training Requirements for all DoD Personnel.** CINCs with geographic responsibilities shall ensure that all DoD personnel entering their AOR have been provided access to AOR-specific information on AT protection.

2.23.1. CINCs, with geographic responsibilities have significant responsibilities for protecting personnel within their AOR. Individuals traveling outside CONUS for either permanent or temporary duty shall have completed annual Level I AT Awareness Training and have received an AOR-specific threat update within three months prior to travel. This information may be provided through multiple means including CINCs publications, messages, and computer home pages. Losing CINCs and/or

Services and/or DOD Agencies shall ensure that personnel departing to another CINC's geographical AOR shall be exposed to and execute the requirements of the gaining CINC's AOR-update.

2.23.2. Furthermore, to enhance the situational awareness and AT preparedness of units prior to transit through and/or deployment to heightened threat areas, gaining CINCs, with geographic responsibilities, shall provide detailed threat information covering transit routes and sites that will be visited by the deployed unit. Such information shall include detailed, focused information on potential terrorist threat (i.e., tailored production and analysis) to aid in the development of tailored AT planning. Since component commanders possess organic intelligence and organic or supporting law enforcement resources, institutional knowledge of their AOR and a comprehensive understanding of unit capabilities, they are best suited to provide such information, when augmented or supported by national and theater assets.

2.23.3. Commanders shall ensure personnel deploying, PCSing, or traveling on leave outside the CONUS receive pre-deployment AT awareness training with a special emphasis on AOR-specific terrorist and medical threats. Commanders shall develop procedures to ensure this training is conducted prior to departing home station and AOR-specific information is incorporated into their pre-deployment AT Level I awareness-training program. AOR-specific threat briefing information for the geographic CINCs can be found on the Internet & SIPRNET sites listed in **Attachment 5**.

**2.24. DoD Standard 24 - Level II Antiterrorism Officer (ATO) Training.** Level II ATO Training is designed to produce an AT advisor to the commander. CINCs and/or Services and/or DoD Agencies shall ensure that each installation and/or deploying unit (i.e., battalion, squadron, ship) is assigned at least one Level II ATO trained individual.

2.24.1. Level II training is designed to qualify individuals assigned as installation ATOs. The training also serves as the primary venue for qualifying AT representatives that deploy forward as AT Advisors. Each AF installation and deploying unit will assign a primary and alternate ATO who will attend Level II training as a minimum standard. While not required, ATOs may also attend courses such as Dynamics of International Terrorism (DIT), Combating Terrorism on Military Installations, and other Service Level II Courses to enhance their proficiency. Level II graduates can also provide Level I training. Each installation requiring Level II training for their assigned ATO or other personnel will schedule training through their MAJCOM/SF or MAJCOM training course IAW MAJCOM instructions. Level II training is open to all career fields.

2.24.2. MAJCOMs who desire to establish their own Level II training programs, will submit a Plan of Instruction to HQ AFSFC/SFP for approval prior to initiating any training.

2.24.2.1. All Air Force Level II programs will use the standardized curriculum based on the requirements for Level II courses found in Table 1.2. MAJCOMs may add command-specific requirements to the core curriculum. MAJCOMs will develop measurable standards for Level II training and determine evaluation methods to ensure trainees are proficient.

2.24.2.1.1. MAJCOMs shall conduct an annual review of their Level II Course Curriculum, using lesson plans developed by the Nov 00, USAF AT Training Workshop to validate minimum curriculum content. HQ AFSFC/SFP maintains the master lesson plans, located on the HQ AFSFC web site, Force Protection Division, AT/FP Training, at **https://wwwmil.lackland.af.mil/afsf/**

2.24.2.1.2. Each Level II course will maintain a reference library of all publications, listed in **Attachment 1** to this publication.

2.24.2.1.3. Each course will develop an AF Form 797 to task certify personnel serving as instructors.

2.24.2.1.4. While not required, each Level II course should add the following capabilities to enhance the effectiveness of their Level II courses:

2.24.2.1.4.1. Consider inviting subject matter experts from agencies such as the FBI, AFOSI, EOD, Medical Group, etc., to brief subject areas. Video teleconferencing should be considered, if available.

2.24.2.1.4.2. Ready access to SIPRNET.

2.24.3. All Level II Training Programs will establish a PDS Code of "AFI" to identify Level II training courses.

2.24.4. MAJCOMs will establish procedures to ensure graduates of their Level II courses are updated in Oracle Training Administrator (OTA) Database.

2.24.5. Personnel serving as Level II Course Instructors will, as a minimum, have completed the following requirements:

2.24.5.1. Completed a formal Air Force instructor's course, such as Principles of Instruction, Academic Instructor School, Basic Instructor Course, etc. The Principles of Instruction course is the minimum required standard.

2.24.5.1.1. Personnel may begin instructing students without having completed this requirement provided they have a certified instructor serving as the Assistant Instructor. However, they are required to have a date to attend one of the above courses within 90 days of assignment of these duties.

2.24.5.2. Be a graduate of an approved Level II Antiterrorism Course listed in **Attachment 7**.

2.24.5.3. Shadow a Level II Certified Instructor as the Level II course is being taught.

2.24.5.4. Be task certified on an AF Form 797.

2.24.5.5. While not required, instructors may also further their AT knowledge by attending courses such as Dynamics of International Terrorism (DIT), Combating Terrorism on Military Installations and other Service Level II courses. Additionally, conducting over-the-shoulder observations of higher headquarters Vulnerability Assessment Teams adds to credibility and subject matter expertise.

2.24.6. Personnel may receive credit for Level II training through any of the following:

2.24.6.1. By attending any of the training courses listed in **Attachment 7** of this instruction.

2.24.6.2. RAVEN graduates prior to Jan 2001 are awarded AT Level II credit based on the curriculum in place prior to the aforementioned date. RAVEN graduates after Jan 2001 are not authorized to perform duties as ATOs or Level I instructors, due to additional training requirements listed in DoDI 2000.16, Table 1.1 and this instruction.

2.24.6.3. USAF personnel, who attend Level II courses conducted by other Services, will receive credit for completing Level II training. These personnel, upon completion of training and return to

home station, will report to the Formal Training Section of their servicing Military Personnel Flight with their Certificate of Training. Formal training will update the individual's completion of training via (OTA) Database.

2.24.7. All AF 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. (RCS: HAF-SFC(AR)0126, Training Reports for Antiterrorism Level I and Level II Training) This report is designated emergency status code C-2. Continue reporting during emergency conditions.

2.24.8. **Table 2.2.** outlines Level II ATO training requirements.

**Table 2.2. Level II ATO Training Requirements.**

| Level of Training | Target Audience | Minimum Training Standard |
|---|---|---|
| Level II AT Officer (ATO)<br><br>Training.<br><br>Graduates shall have requisite knowledge and materials to manage a comprehensive AT Program and advise the commander in all AT areas. | Officers/NCOs/ civilian staff officers, who are coded, tracked and command-designated to serve as the AT advisor to the commander and provide Level I instruction. | 1. Service-provided instruction (resident or MTT); incorporates Service-standardized POI consisting of the following minimum topics:<br>Understanding AT Roles and Responsibilities<br>- Understand Policy & Standards<br>- Access Reference Sources<br>Organize for AT<br>- Command/Staff Relationships<br>- FP Working Groups<br>Assess Vulnerabilities<br>- Baseline Unit FP Posture Conduct Assessment (Practical Exercise)<br>Assess Threat<br>- Intel / CI Integration<br>- Information Operations<br>Create and Execute AT Programs<br>- Use of Terrorism Threat Level/ FPCONS<br>- Unit/Installation Protective Measures<br>- Mitigating Vulnerabilities<br>Prepare AT Plans<br>- Templates & Planning Tools<br>- How to Develop & Write Plans<br>- WMD Considerations<br>- Use of RAM to protect the<br>- Installation<br>AT Resource Management<br>- Requirements Generation & Prioritization<br>- CbTRIF<br>Conduct AT Training<br>- Exercise Unit AT Plans<br>- Obtain AOR-specific updates<br>- Oversee AT Level I Training<br>2. Review of DoD O-2000.12/12H, DoDI 2000.16 and other applicable DoD/Service/ Agency publications.<br>3. Methods available for obtaining AOR-specific updates for deployment/travel areas.<br>4. Service-directed modules on other aspects of AT, such as physical security requirements, technology updates, etc. |

2.24.9. Level III Pre-Command AT Training. Level III Pre-Command AT Training is designed to expose the prospective commander to AT issues. Services and/or DoD Agencies shall ensure that pre-command training tracks provide Level III Pre-Command AT Training to prospective commanders. In particular, this training shall be tailored to provide prospective commanders the depth and breadth necessary to perform the full spectrum of AT responsibilities.

2.24.9.1. AF Level III 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.

2.24.9.2. MAJCOM/SF directors will determine minimum qualifications for personnel delivering Level III training within their MAJCOM.

2.24.9.3. MAJCOMs will determine procedures for delivering Level III training to personnel who are not able to attend the MAJCOM Commanders Orientation Course.

2.24.9.4. **Table 2.3.** Outlines Level III Pre-Command AT Training requirements.

**Table 2.3. Level III Pre-Command AT Training Requirements.**

| Level of Training | Target Audience | Minimum Training Standard |
|---|---|---|
| Level III Pre-Command AT Training.<br><br>Graduates shall have requisite knowledge and materials to supervise a comprehensive AT Program and manage AT issues. | O-3 to O-6 commanders<br>**MAJCOMs are encouraged to have vice commanders and deputy commanders Level III trained. | MAJCOM-provided instruction during pre-command pipelines; incorporates USAF-standardized POI consisting of the following minimum topics:<br><br>1. Viewing the SECDEF/CJCS Video<br><br>2. Directive/reference review<br>Understand AT Responsibilities<br>- Understanding Policy<br>- Vulnerability Assessments (VAs)<br>- Food and Water Vulnerability<br>- Off-Installation Housing<br><br>Ensure Preparation of AT Plans<br>- Baseline FP Posture<br>- Mitigating WMD Attack<br>- -MOUs/MOAs<br><br>Ensure Conduct of AT Planning<br>- AT Plans & Training<br>- Level I Training<br><br>Organize for AT<br>Understand the Local Threat Picture<br>- Fusion of Intelligence<br><br>Building a Sustainable AT Program<br>- Terrorism Threat Levels<br><br>Executing Resource Responsibilities<br>- AT Resource Programs<br>- Construction Standards<br>Understanding Use of Force and ROE<br>- Terrorist Scenarios & Hostile Intent Decision Making.<br><br>2. Review of DoD INSTs 2000.12, 2000. O 12-H, 2000.16 and other applicable DoD/ Service/Agency publications.<br><br>3. Issuance of Commander's Handbook (Joint Pub 5260). |

2.24.10. Level IV AT Executive Seminar. The Level IV AT Executive Seminar is designed to expose senior officers in the grade of O-6 through O-8 and DoD civilians equivalent in grades to AT issues.

2.24.10.1. AF Level IV Executive-Level Commander Training is accomplished by the Combating Terrorism Directorate of the Joint Staff (J34). It is designed for installation commanders, Joint Task Force (JTF)/Battle Group level commanders, and those responsible for AT policy, planning and execution. Once training quotas are established through J34, 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.

2.24.10.2. **Table 2.4.** Outlines Level IV AT Executive Seminar training requirements.

**Table 2.4. Level IV Executive Seminar Training Requirements.**

| Level of Training | Target Audience | Minimum Training Standard |
|---|---|---|
| Level IV AT Executive Seminar.<br>** Graduates shall have requisite knowledge and materials to provide oversight to AT Programs and Policies. | Officers in the grade of O-6 to O-8 and DoD civilians in equivalent grades selected by Service/ CINC/DoD Agencies who are responsible for AT programs or involved in AT policy, planning and execution. | CJCS Executive-level seminar hosted by J-34. Provides pertinent current updates, briefings, and panel discussion topics. Seminar includes three tabletop AT war games aimed at facilitating interaction and discussion among seminar participants. |

2.24.11. Commanders at all levels, who receive individuals that are not properly trained, shall, in the interest of force protection, provide the required AT training as soon as practicable upon the gain. Concurrently, they shall report the deficiency through their DoD component chain of command. The DoD component shall subsequently notify the providing commander and ensure appropriate measures are generated to prevent reoccurrence of the discrepancy.

**2.25. DoD Standard 25 - Training for High-Risk Personnel and High-Risk Billets.** CINCs and/or Services and/or DoD Agency Heads have been given substantial AT responsibilities for DoD personnel assigned to high-risk billets or at high risk to terrorist attacks. High-risk personnel are eligible for advanced AT training. In some instances, this training may be extended to include family members.

2.25.1. The Services and DoD Agency Heads shall ensure personnel designated as “Personnel at High-Risk to Terrorist Attack” and “Personnel Assigned to High-Risk Billets” receive appropriate training. To this end, CINCs with geographic responsibilities shall communicate high-risk positions and high-risk personnel to their Service authority for AT, not less than annually to enable the Services to provide for the requisite training. Whenever possible, the Services should conduct the appropriate AT training of designated personnel prior to arrival in theater.

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

2.25.3. Travel of high-risk personnel. When the threat dictates, commanders shall restrict details of the travel arrangements for high-risk individuals or senior officials (general officer or civilian equiva-

lent) to reduce the vulnerability to attack. Unless absolutely necessary for travel security, do not stop public announcements of special events, guest speakers or other ceremonies senior officials attend. Make such announcements without divulging the specific travel itinerary or local arrangements.

2.25.4. Itineraries for high-risk billeted personnel and personnel susceptible to terrorist attacks shall, at a minimum, be marked 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.

2.25.5. During increased FPCONs, residential and travel security of assigned or visiting high- risk personnel or other probable terrorist targets, should be increased to counter the threat. Ensure these personnel receive timely security awareness briefings. For the most serious cases, request protective services from AFOSI. AFOSI will provide protective services, including long-term protective service operations (PSO), when specific, credible threats exist and when the requester and AFOSI jointly determine such protection is needed.

**2.26. DoD Standard 26 - Vulnerability Assessment of Installations.**

2.26.1. Assessment Focus. Vulnerability assessment shall focus on the assessed installation overarching AT program. AT programs should be subject to continual assessment to avoid complacency and gain benefit from experience 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 assessment essential. VAs will normally occur at the installation commander level and above; however, because VAs are critical to forces transiting through ports, airfields, and inland movement routes, geographic CINCs shall ensure component commanders conduct VAs frequently enough to ensure timely and accurate information is available. These assessments should consider the range of identified and projected terrorism threats against a specific location or installation, personnel, family members, facilities and other assets. The assessment should identify vulnerabilities and solutions for enhanced protection of DoD personnel and resources.

2.26.1.1. AT Assessment Functional Areas. AT VAs provide a vulnerability-based analysis of an activity's AT program. The assessment identifies, for the commander, vulnerabilities that may be exploited by terrorists and suggests options that may eliminate or mitigate those vulnerabilities. The assessment team shall evaluate the installations overall AT Awareness posture IAW Table 1.1 of this instruction and DoDI 2000.16, Standard 22, table 1.1.

2.26.1.2. All VAs will be classified in accordance with the DTRA Security Classification Guide.

2.26.2. There are two types of VAs: the local VA and the higher headquarters VA.

2.26.2.1. Installation commanders shall have the ATO form a multi-functional VA team (i.e., AFOSI, CE, SV, SF, IN, SC, MG, etc.) to conduct the local VA. The VA shall address the full spectrum of threats to mission-essential critical infrastructures and assets, security of personnel, physical threats and installation infrastructures. Utilities, facilities with large populations, food, water, fire protection, medical response, communication centers, etc., shall all be addressed in the assessment. The assessment shall provide solutions for enhanced protection of DoD personnel and resources. Installation commanders shall forward copies of the VA to their NAF and MAJCOM to help coordinate resource allocation and advocacy.

2.26.2.1.1. Local VAs shall be conducted at least annually, except for those years when a higher headquarters VA is conducted.

2.26.3. Higher Headquarters (HHQ) VAs. CINCs/Services/Agencies shall ensure lower level AT Programs receive a HHQ VA, at least once every three years, to ensure unity of AT efforts throughout their subordinate commands. Each CINC, Service Chief and DoD Agency Director shall track and identify vulnerabilities throughout the chain of command. As a minimum, each commander or director shall prioritize, track and report to the next general/flag officer, the action to be taken to address vulnerabilities identified in the vulnerability assessment.

2.26.3.1. Installation commanders shall work with their MAJCOM to ensure they receive such assessments once every three years as a minimum, or as specified by the CINC with responsibility for the AOR. To provide essential visibility, as a minimum, installation commanders shall prioritize, track and report the vulnerabilities identified to the next general officer or equivalent and the action taken following the VA.

2.26.4. JSIVA, AF or MAJCOM VA Teams shall accomplish HHQ VAs. Each of these agencies may conduct independent or joint assessments. The Air Force VA Team (VAT) may also conduct "over-the-shoulder" observations of MAJCOM assessments and conduct other assessments, as directed by AF/XOF or the Air Staff FPWG. MAJCOMs may establish a team to conduct the assessments and, if established, shall provide a copy of their assessment schedule to AFSFC/SFP by 15 September annually. Installations scheduled to receive AF VAs shall provide the information requested in **Attachment 6** of this instruction to HQ AFSFC/SFP NLT 30 days prior to their scheduled assessment by way of e-mail.

2.26.5. HHQ VA Scheduling. MAJCOM SFs are responsible for keeping track of the frequency and scheduling of VAs for their subordinate installations. HQs AFSFC schedules HHQ VAs contingent on input from the MAJCOM SF. This process is accomplished once a year with candidate installation input provided from the MAJCOM SF to HQ AFSFC. HQ AFSFC will request VA nominees by 15 September of the calendar year preceding the calendar year of the assessment.

2.26.6. HHQ VAs satisfies the annual requirement for Local VAs.

2.26.7. VA Site Criteria. HHQ VAs shall be conducted at DoD components, housing areas, facilities and/or activities/locations and command levels identified as "installations." For the purposes of this instruction, the following defines an assessment-eligible installation:

2.26.7.1. Any DoD facility consisting of 300 or more personnel on a daily basis.

2.26.7.2. Any DoD facility bearing responsibility for emergency response and physical security plans and programs.

2.26.7.3. Any DoD facility possessing authority to interact with local non-military or host nation agencies or having agreements with other agencies or host nation agencies to procure these services.

2.26.7.4. HHQ VAs may be conducted at any DoD Component Activity, when CINCs, and/or Services and/or Agencies identify a time critical requirement or emergent need.

2.26.8. VAs conducted to meet the requirement contained in this standard must assess as a minimum, the following functional areas:

2.26.8.1. AT Plans and Programs. The assessment shall examine the assessed installation's/activity's AT program and ability to accomplish appropriate standards contained in DoDI 2000.16, this AFI, and applicable prescriptive standards established by the appropriate CINC/Service/Agency.

2.26.8.1.1. The assessment shall examine written plans in the areas of counterintelligence, law enforcement liaison, intelligence support, security and post-incident response (the ability of the installation/activity to respond to terrorist incidents, especially mass casualty events, to include a disease outbreak caused by terrorist use of a biological weapon).

2.26.8.1.2. The assessment shall examine the degree to which plans complement one another and support the assessed installation's/activity's ability to identify changes in the terrorist threat, react to threat changes by implementing appropriate AT measures and provide appropriate responses should a terrorist event occur.

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

2.26.8.2. Counterintelligence, Law Enforcement Liaison and Intelligence Support. The assessment shall focus on an installation's/activity's ability to receive threat information and warnings from HHQ and local resources, actively collect information on the threat (when permitted), process that information to include local fusion and analysis, and develop a reasonable postulated threat statement of the activity. The assessment shall also examine an installation's/activity's ability to disseminate threat information to subordinate commands, tenant organizations, in-transit units, geographically separated units and assigned or visiting DoD personnel (including military members, civilian and contractor employees and family members). The assessment shall also examine how the process supports the implementation of appropriate force protection measures to protect military personnel, DoD civilians, and family members.

2.26.8.2.1. The assessment shall focus on the most probable terrorist threat for the installation/activity and appropriate countermeasures. In cases where no identified threat exists, the installation/activity shall be assessed on their ability to implement AT measures under increasing FPCONs, in response to increased terrorist threat levels or terrorist threat warnings.

2.26.8.3. AT Physical Security Measures. The assessment shall determine the assessed installation's/activity's ability to protect personnel by detecting or deterring terrorists, and failing that, to protect by delaying or defending against terrorist acts. Physical security techniques include procedural measures such, as perimeter security, security force training, security surveys, medical surveillance for unnatural disease outbreaks and armed response to warning or detection. The assessment shall also determine physical security measures such as fences, lights, food and water, intrusion detection devices, access control systems, closed circuit television cameras, personnel (to include Resource Augmentation Duty (READY), vehicle barriers, biological, chemical and radiological agent detectors and filters, and other security systems effectiveness. The assessment shall consider commercial, off-the-shelf AT technology enhancements and potential solutions for those circumstances where existing technology or procedural modifications do not provide satisfactory solutions.

2.26.8.4. Vulnerability to a Threat and Terrorist Incident Response Measures. The assessment shall examine the assessed installation's/activity's ability to determine its vulnerabilities against commonly used terrorist weapons and explosive devices, to include terrorist use of WMD. The assessment shall 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, shall also be examined.

2.26.8.5. VAs for Terrorist Use of WMD. The assessment shall assess the vulnerability of installations, facilities and personnel, and family members within their AOR to terrorist use of WMD. Such assessments address potential use of chemical, biological, nuclear or radiological agents and shall be developed with supporting base agencies, such as civil engineering, readiness, medical, etc.

2.26.8.6. Host Nation, Local Community, Inter-Service and Tenant Support. The assessment shall examine the level and adequacy of support available to an installation/activity from the host nation or local community, MAJCOM, HQ USAF and where appropriate, inter-service and tenant organizations to enhance AT measures or response to terrorist incidents.

2.26.8.6.1. The assessment shall determine the integration and feasibility of plans with 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 response to terrorist events, with emphasis on mass casualty situations.

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

2.26.8.6.3. The assessment shall determine the status of formal agreements with supporting organizations by way of Memorandums of Understanding or Agreement, Inter-Service Support Agreements and Host Tenant Support Agreements, or other methods.

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

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

2.26.10.1. Force Protection Integrated Support Team (FIST). Based on site-specific factors such as a Terrorism Threat Level, terrorist characteristics, geography or emergent force protection challenges, specialized assessment teams may be commissioned with expertise to address a commander's force protection posture. One such team is the AFSFC's Force protection Integrated Support Team. The FIST is charged to mitigate or solve emergent USAF-wide AT/FP requirements. Team expertise may include: AT technology; explosive ordinance disposal; communications; information assurance or operations and other specialties as determined by the CINC, Service, DoD Agency or MAJCOM sponsoring the assessment. Requests for FIST support should pass through command channels to HQ AFSFC/SFP, DSN 473-0896, or through the 24-hour AFSFC Operations Center, DSN 473-0960.

2.26.11. HQ AFSFC shall disseminate lessons learned, trends and best practices to MAJCOMs for their use and further dissemination.

2.26.12. Air Force units will use the Air Force Vulnerability Assessment Management Program (VAMP) to comply with DoD tracking and report requirements. VAMP is a web-based program accessed through the SIPRNET. HQ Air Force Security Forces Center, Force Protection Division (AFSPC/SFP) is the VAMP Program Manager. MAJCOMs and installations will appoint VAMP Administrators and notify AFSFC/SFP of the appointee.

2.26.13. The Air Force VA Guide is the source document for all Air Force (local, MAJCOM & AF) VAs. Vulnerabilities identified during the VA outbrief are to be entered into VAMP NLT 10 duty days after the VA outbrief. Observations, concerns, and best practices identified by the VA team will be entered into VAMP NLT 30 duty days following the receipt of the final VA report.

2.26.14. A color-coded rating scheme will be used by MAJCOM and installations to give visibility to vulnerabilities and to facilitate tracking of corrective actions. Following the receipt of a DoD, AF, MAJCOM or local VA report, the installation commander must determine the baseline color-code rating using the Critical Program Requirements listed in **2.26.14.** Failure to achieve a "GO" rating in any of the Critical Program Requirement areas will result in an overall "Red" rating.

2.26.14.1. The color-code denotes an installation or agency's overall assessment status: Red - AT/FP practices and procedures do not adequately address the current local threat level; AMBER - AT/FP practices and procedures are marginally acceptable given the current local threat level; GREEN - AT/FP practices and procedures are satisfactory given the current local threat level.

2.26.14.2. Those installations that commanders have assessed as RED will require a reassessment with six months after the original assessment. The appropriate HHQ will determine the type and scope of assessment required. If the vulnerabilities identified, that drove the RED rating, can't be corrected at the time of the reassessment, the appropriate HHQ will be notified and will determine if a HHQ assessment is required for that location. Once the identified vulnerability areas have been corrected, commanders will reevaluate their installation's AT/FP readiness and assign a new color-rating.

2.26.15. There are nine Critical Program Requirements which all installations and agencies must meet to satisfy the basic AT/FP program standards promulgated by DoD. The nine standards are:

2.26.15.1. Comprehensive AT/FP Program Established and Maintained. (Standards 2 and 14)

2.26.15.2. Trained AT Officer (AT)) Assigned in Writing. (Standard 6)

2.26.15.3. Local Threat Assessment Conducted Within Last 12 Months. (Standard 15)

2.26.15.4. Threat Information Notification System Established. (Standard 9)

2.26.15.5. Comprehensive Local Vulnerability Assessment and Program Review Completed Annually. (Standards 20 and 26)

2.26.15.6. Signed, Distributed, Executable AT/FP Plan Fully Coordinated with Tasked Units. (Standard 14)

2.26.15.7. At/FP Plan Exercised Annually and Lessons Learned Documented. Standard 19)

2.26.15.8. Countermeasures in Place to Mitigate Known Vulnerabilities. (Standard 14)

2.26.15.9. Adoption/Adherence to "Interim DoD AT/FP Construction Standards." (Standard 28)

2.26.16. VAMP access is controlled and limited to a "need to know" basis. Access will be requested through and revalidated semi-annually by the AFSFC VAMP Program Manager and MAJCOM

VAMP Administrators. The below listed positions have been identified with a continuing need for access to VAMP:

2.26.16.1. AF/XO and AF/XOO staff divisions, as appropriate.

2.26.16.2. Director of Security Forces (AF/XOF)

2.26.16.3. Commander, HQ AFSFC (AFSFC/CC)

2.26.16.4. Chief, Force Protection Division (AFSFC/SFP)

2.26.16.5. MAJCOM Commanders, SF Directors, and VAMP Administrators or designated representatives.

2.26.16.6. Installation Commanders and VAMP Administrators

2.26.17. MAJCOM and Installation VAMP Administrators will strictly monitor the number of personnel who have access to VAMP. MAJCOM VAMP Program Administrators are responsible for accuracy of data entered into VAMP and will ensure Installation VAMP Administrators are trained.

2.26.18. VAMP Program Manager is responsible for training MAJCOM VAMP Administrators.

2.26.19. USAF Strategic Plan Performance Measures. MAJCOMs will report the VA status of their respective installations to HQ USAF/XOFP NLT 15 Oct and 15 Apr of each year, IAW with Air Force Strategic Plan, Volume 2, Performance Measure 2.A.13, Antiterrorism/Force Protection Program Assessments. (This vulnerability assessment status reporting requirement is exempt from report control symbol (RCS) licensing in accordance with AFI 33-324, paragraph 2.11.1, *The Information Collections and Reports Management Program*).

2.26.19.1. Further details regarding this Performance Measure can be found at **https://www.afmia.randolph.af.mil/afmia/mip/mipp/perf_mgt/ppm.htm**

**2.27. DoD Standard 27 - Pre-deployment AT Vulnerability Assessment.** DoD Components shall ensure the execution of pre-deployment AT VA prior to deployment. At the theater level, Component Commanders shall provide onboard and/or advance-site assessments prior to and during visits to higher-threat areas of Significant or High Threat Levels, or where a geographically specific Terrorism Warning Report is in effect. This includes ports, airfields and inland movement routes that may be used by transiting forces. At the discretion of the geographic CINC, such security efforts may be waived for deployments and/or visits to controlled locations such as existing military installations or ships afloat. Augmentation of assessment personnel may be necessary to enable Component Commanders to discharge their responsibility to provide security, surveys and assessments, counterintelligence and countersurveillance support and to act as the liaison with the country team, host nation security force, husbanding contractor and port authority. Such advance-site deployment would also be able to communicate current local threat information to transiting units, enabling the onboard AT team to more effectively tailor measures to the specific threat environment.

2.27.1. Deploying commanders shall implement appropriate AT measures to reduce risk and vulnerability. Commanders shall direct implementation of AT measures that reduce risks before, during and after deployment. Assessments and the subsequent implementation of standards must occur in a timely manner and should 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.

2.27.1.1. If warranted, commanders faced with emergent AT and force protection requirements prior to movement of forces, should submit CbTRIF requests through established channels to procure necessary materials or equipment for required protective measures.

2.27.1.2. Equipment and technology can significantly enhance all DoD forces, but in particular the transiting units' posture against terrorist threats. For this reason, component commanders should research and identify AT equipment or technology requirements to their chain of command. The use of commercial-off-the shelf or government-off-the-shelf products should be stressed to meet near-term requirements.

2.27.2. The senior deploying commander will ensure a pre-deployment VA has been conducted and a counterintelligence threat assessment provided by AFOSI prior to deployment. The assessment team will include medical members qualified to conduct site selection evaluations to include: vulnerability of local food and water sources, medical threats, , local medical capabilities, vector/pest risk assessment, field sanitation and of hygiene of local billeting and public facilities, and 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.

2.27.3. Servicing AFOSI detachments will provide a threat assessment for any deployments to the supported installation

2.27.4. The command intelligence officer will ensure the commander and key unit personnel possess appropriate sensitive compartmented information (SCI) clearances and have access to communications to receive urgent threat information at the deployed location.

**2.28. DoD Standard 28 - Construction Considerations.** DoD Components shall adopt and adhere to common criteria and minimum construction (i.e., new construction, renovation, or rehabilitation) standards to mitigate AT vulnerabilities and terrorist threats.

2.28.1. The Air Force Civil Engineer (AF/ILE) shall develop construction guidelines IAW DoD O-2000.12-H. The guidelines shall cover antiterrorism planning, design, refurbishment and construction (MILCON) of all Air Force facilities to reduce the vulnerability of Air Force personnel to terrorist attacks. At a minimum, they will meet the 16 Dec 99 Interim DoD AT/FP Construction Standards.

2.28.2. 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.

2.28.2.1. Installation commanders shall ensure all new construction projects and applicable renovation projects, regardless of the funding source, employ AT features and meet minimum DoD AT Construction Standards.

2.28.2.2. Construction of temporary/expeditionary structures. For temporary and expeditionary discussions refer to Air Force Handbook 10-222, Volume 3. Commanders are also expected to use expeditionary measures commensurate with the identified FPCON.

2.28.2.3. The Base Civil Engineer shall coordinate security requirements with the installation ATO on all facility construction and rehabilitation projects to ensure compliance with AT criteria

and resource protection/AFOSI input/coordination. The installation ATO shall ensure all facility related AT/FP enhancements (i.e., fences, bollards, barriers, barricades, etc.) funded by the AT/FP program funds are coordinated with the Base Civil Engineer and MAJCOM CE. At a minimum, these efforts should be documented on an Air Force Form 332, Civil Engineer Work Request.

2.28.2.3.1. All waivers to this criteria will be considered on a case-by-case basis and must be approved by HQ/ILEC.

**2.29. DoD Standard 29 - Facility and Site Evaluation and/or Selection Criteria.** Commanders shall develop a prioritized list of AT 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. Circumstances may require the movement of DoD personnel or assets to facilities the US government has not previously used or surveyed. AT standards should be a key consideration in evaluating the suitability of these facilities for use.

2.29.1. The servicing AFOSI detachment, medical, intelligence, security forces and civil engineers, as a minimum, will participate in the site selection process.

**2.30. DoD Standard 30 - AT Guidance for Off-Installation Housing.** Commanders shall ensure DoD personnel assigned to Moderate, Significant or High Terrorist Threat Level areas, who are not provided on-installation or other government quarters, are furnished guidance on the selection of private residences to mitigate risk of terrorist attack. The best protection for individuals is an awareness of the threat and the willingness to take steps necessary to reduce threat exposure.

2.30.1. Residential Security Reviews for Off-Installation Housing. Commanders, in Significant or High Terrorist Threat Level areas, shall conduct physical security reviews of off-installation residences for permanently assigned and temporary-duty DOD personnel. Such reviews shall 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 for which they have AT responsibility.

2.30.1.1. Such reviews shall be conducted at least annually.

2.30.1.2. Based on the review results, commanders shall provide AT recommendations to residents and facility owners, facilitate additional mitigating measures, and as appropriate, recommend to appropriate authorities the construction of on-installation housing or lease of housing in safer areas.

2.30.2. Commanders shall complete residential security reviews, in Significant or High Terrorist Threat Level areas, prior to personnel entering into formal contract negotiations for the lease or purchase of off-installation housing. Residences overseas are more apt to install security enhancements prior to the entering into a contract.

2.30.2.1. 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 Moderate, Significant or High Terrorist Threat Levels. This guidance provides information as to selection of homes to minimize the risk of terrorist acts.

2.30.3. Installation commanders assigned to Low or Moderate Terrorist Threat Level areas will evaluate the need to conduct assessments of off-installation housing areas.

2.30.4. Use the VA process outlined in paragraph **2.26.** to ensure proper assessment of off-installation housing, if deemed necessary.

2.30.5. Commanders shall include coverage of private residential housing in AT plans where private residential housing must be used in Moderate, Significant or High Terrorist Threat Level areas.

2.30.6. 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 personnel threat exposure.

2.30.7. Commanders, at all levels, should incorporate family member and dependent vulnerabilities into all AT assessment, mitigation and reporting tools. In Moderate, Significant or High Threat areas, commanders shall include coverage of facilities (i.e., DoD schools and child development centers) and transportation services and routes (i.e., bus routes) used by DoD employees and their family members.

**2.31. DoD Standard 31 - Executive Protection and High Risk Personnel Security.** Commanders shall be familiar with treaty, statutory, policy, regulatory and local constraints on the application of supplemental security measures for certain high-ranking DoD officials whom are entitled to additional protection as a result of their position. Commanders shall take measures necessary to provide appropriate protective services for such individuals in high-risk billets and high-risk personnel. Review and revalidation of protective services shall occur on at least an annual basis.

2.31.1. 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 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.

2.31.2. Reviews of supplemental security needs should be undertaken within 30 days of a change in the Terrorism Threat Level assigned to an AOR containing high-risk billets or to which high-risk personnel have been assigned.

2.31.3. HQ AFOSI provides special AT training including the Protective Service Operation/AT 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.

**2.32. Associated Standards from DoD O-2000.12-H. Table A2.1.** In **Attachment 2** associates standards from this instruction with the existing DoD O-2000.12-H. Use this handbook as guidance to implement the installation AT program.

CHARLES F. WALD, Lt General, USAF
DCS/Air and Space Operations

## Attachment 1

## GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

***References***

CJSCI 5261.01, Chairman of the Joint Chiefs of Staff Instruction, *Combating Terrorism Readiness Initiatives Fund*

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 Directive 5240.1, DoD Intelligence Activities*

*DoD Directive 5240.2, DoD Counterintelligence*

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

DoD Instruction 2000.16, *DoD Antiterrorism Standards*

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

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

DoD Regulation 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons*

*Executive Order 12333, US Intelligence Activities*

*H.R.. 3162, 'Uniting and Supporting Information by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) of 2001*

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

*Joint Pub 2-01.2, Joint Doctrine , Tactics, Techniques, and Procedures for Counterintelligence Support to Operations*

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*

*United States Air Force Foreign Clearance Guide*

*AFMD 39, Air Force Office of Special Investigations*

*AFMAN 10-100, Airman's Manual*

AFMAN 10-206, *Operational Reporting*

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

*AFH 10-222, USAF Weapons of Mass Destruction Threat Planning and Response Handbook*

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

*AFH 10-2502, WMD Terrorist Threat Planning and Response Operations*

*AFI 10-2601, Counter-NBC, Passive Defense*

*AFI 10-2602, NBCC Defense Operations and Standards*

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

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

AFI 31-207, *Arming and Use of Force by Air Force personnel*

*AFI 71-101, Vol. 2, Protective Service Matters*

*AFI 71-101, Vol. 4, Counterintelligence*

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

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

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 Flight 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 71-1, Criminal Investigations and Counterintelligence*

AFI 35-101*, Public Affairs Policies and Procedures*

AFI 36-2201, *Air Force Training Program*

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

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

*AFI 41-106, Medical Readiness Planning and Training*

AFI 48-101, *Aerospace Medical Operations*

AFI 48-116, *Food Safety Program*

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

AFMAN 32-10138, *Military Construction Planning and Programming Manual***,** *Air Force Center for Environmental Excellence (AFCEE) Installation Force Protection Guide*

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

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

*Interim Department of Defense Antiterrorism/Force Protection (AT/FP) Construction Standards Memorandum, December 16, 1999*

MEDIC CD ROM, *Medical Environmental Disease Intelligence and Countermeasures, Armed Forces Medical Intelligence Center, Ft. Detrick, MD*

*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

*Food and Water Systems Force Protection Guidelines, Air Force Medical Operations Agency, Bolling AFB, DC*

*Defense Threat Reduction Agency (DTRA) Classification Guide*

DTRA checklists for Vulnerability Assessments

DoD Antiterrorism Construction Standards

***Abbreviations and Acronyms***

**AFSFC—**Air Force Security Forces Center

**AT—**Antiterrorism

**ATO—**Antiterrorism Officer

**CBRNE—**Chemical, biological, radiological, nuclear materials or high-yield explosive device

**CbTRIF—**Combating Terrorism Readiness Initiatives Fund

**CI—**Counterintelligence

**CS—**Countersurveillance

**DIA—**Defense Intelligence Agency

**DoS—**Department of State

**DRU—**Direct Reporting Unit

**DTRA—**Defense Threat Reduction Agency

**EOD—**Explosive Ordinance Disposal

**FAA—**Federal Aviation Administration

**FIST—**Force Protection Integrated Support Team

**FOA-—**Forward Operating Agency

**FP—**Force Protection

**FPCON—**Force Protection Condition

**FPSG—**Force Protection Steering Group

**FPWG—**Force Protection Working Group

**NBC—**Nuclear, Biological or Chemical

**POM—**Program Objective Memorandum

**PSO—**Protective Service Operations

**RAM—**Random Antiterrorism Measure

**TCM—**Terrorism Consequence Management

**TWG—**Threat Working Group

**WMD—**Weapons of Mass Destruction

**VA—**Vulnerability Assessment

**VAMP—**Vulnerability Assessment Management Program

**VAT—**Vulnerability Assessment Team

***Terms***

**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)

**Antiterrorism Officer/NCO (ATO)—**The installation , base, regional, facility, or deploying AT advisor charged with managing the AT Program. He/she shall be a graduate of an approved Level II Course and be identified in writing by the installation and/or force commander.

**Antiterrorism Plan (AT Plan)—**An AT Plan is the specific measures taken to establish and maintain an AT Program.

**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.

**Combating Terrorism—**Combating terrorism within the DoD encompasses all actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts), counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism), terrorism consequence management (preparation for and response to the consequences of a terrorist incident/event), and intelligence support (collection and dissemination of terrorism-related information) taken to oppose terrorism throughout the entire threat spectrum, to include terrorist use of chemical, biological, radiological, nuclear materials or high-yield explosive devices (CBRNE).

**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 Analysis—**CI analysis is the function of assimilating, evaluating, and interpreting information about areas of CI prepotency and responsibility. Information derived from all available sources is considered and integrated in the analytical process.

**Counterintelligence Collection—**The systematic acquisition of information (through investigations, operations, or liaison) concerning espionage, sabotage, terrorism, other intelligence activities or

assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign person.

**Counterintelligence Investigation—**Counterintelligence investigations establish the elements of proof for prosecution or administrative action. Counterintelligence investigations can provide a basis for or be developed from conducting counterintelligence operations. Counterintelligence investigations are conducted against individuals or groups suspected of committing acts of espionage, sabotage, sedition, subversion, terrorism, and other major security violations as well as failure to follow defense agency and Military Service directives governing reporting of contacts with foreign citizens and "out-of-channel" requests for defense information. Counterintelligence investigations provide military commanders and policy makers with information used to eliminate security vulnerabilities and otherwise to improve the security posture of threatened interests.

**Counterintelligence Operation—**Actions taken against foreign intelligence services to counter espionage and other clandestine intelligence activities damaging to the national security.

**Counterintelligence Production—**The process of analyzing all source information concerning espionage or other multidiscipline intelligence collection threats, sabotage, terrorism, and other related threats to US military commanders, the Department of Defense, and the US Intelligence Community and developing it into a final product that is disseminated. Counterintelligence production is used in formulating security policy, plans, and operations.

**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)

**Countersurveillance—**All measures, active or passive, taken to counteract hostile surveillance.

**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)

**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)). (DoDD 2000.12)

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

**Environmental Threat Assessment—**Multimedia medical assessment for biological, chemical, physical and radiological hazards at an established installation or at a deployment site.

**Food and Water Vulnerability—**The susceptibility to overt/covert attack of food and water assets or sources that could cause incapacitation or death of personnel.

**Force Protection—**Commander's program designed to protect Service members, civilian employees, family members, facilities, information 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)

**Force Protection Conditions (FPCONs)—**A DoD-approved system standardizing the DoD and Military Services' identification of and recommended preventive actions and responses to terrorist threats against US personnel and facilities. The system is the principle means for a commander to apply an operational decision on how to protect against terrorism and facilitates inter-Service coordination and support for antiterrorism activities. Also called FPCONs. There are four FPCONs above normal:

**FPCON NORMAL—**This condition applies when a general global threat of possible terrorist activity exists and warrants a routine security posture.

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

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

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

**FPCON DELTA—**Applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is imminent. Normally, this FPCON is declared as a localized condition. (Joint Pub 1-02)

**Force Protection Integrated Support Team (FIST)—**The FIST is a dedicated team tasked to respond to a MAJCOM's or installation commander's request to mitigate or solve emergent USAF-wide AT issues that cannot be resolved internally.

**Force Protection Working Group (FPWG) —**The FPWG is the commander's cross-functional working group made up of wing and tenant units. Working group members are responsible for coordinating and providing deliberate planning for all antiterrorism/force protection issues. The FPWG should include representatives from relevant disciplines across the installation, including civil engineering, intelligence, AFOSI, security forces, public health, bioenvironmental, disaster preparedness, plans, communications and other agencies the installation commander deems necessary, including tenant units

**Foreign Intelligence—**Information relating to the capabilities, intentions, or activities of foreign powers, organizations, or persons, but not including counterintelligence, except for information on international terrorist activities.

**Forensic Sciences Consultant—**AFOSI special agents who receive thorough graduate-level training in most aspects of the forensic sciences and further specialization in a variety of forensic areas, to include Federal Bureau of Investigations post-bomb blast investigations. These specially trained agents provide support ranging from reviewing major investigation and advising on the use of specialized forensic

techniques, to providing on-scene operational assistance in investigations.

**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, lodging, dormitories, 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.

**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)

**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.

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

**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)

**Protective Services—**A specialized AFOSI activity which increases the personal safety and security of distinguished visitor or other protectee. The activity may be limited to protective threat assessment or may

extend to a major protective service operation involving considerable manpower and resources ( AFI 71-101, Vol. 2).

**Protective Service Operation (PSO)—**The use of specialized techniques and procedures by AFOSI personnel to ensure a protectee's personal safety and security during a specific event, while traveling, or over an extended period of time. When required, a PSO can be tailored to provide 24-hour protection. In such cases, the security detail establishes defensive overt or clandestine perimeters around the protectee for the term of the PSO at the residence, during travel, and at all sites on the protectee's daily itinerary. (AFI 71-101, Vol 2)

**Protective Threat Assessment (PTA)—**Collecting and analyzing information to identify direct any potential threats to harm, seize, interfere with, or embarrass a specific protectee, as well as to determine the existing and anticipated security environment. A PTA is always the initial phase of a PSO. (AFI 71-101, Vol 2)

**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)

**Terrorism Consequence Management (TCM)—**DoD preparedness and response for mitigating the consequences of a terrorist incident including the use of a weapon of mass destruction. DoD consequence management activities are designed to support the lead federal agency (domestically, FEMA; overseas, DoS) and include measures to alleviate damage, loss of life, hardship or suffering caused by the incident; protect public health and safety; and restore emergency essential government services.

**Terrorism Threat Analysis—**In antiterrorism, threat analysis is a continual process of compiling and examining all available information concerning potential terrorist activists by groups that could target a facility. A threat analysis will review factors of the presence of a terrorist group, operational capability, activity, intentions and operating environment.

**Terrorism Threat Assessment—**The process used to conduct a threat analysis and develop an evaluation of a potential terrorist threat and the product of a threat analysis for a particular unit, installation or activity.

**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, that commits acts of violence or threatens violence in pursuit of its political, religious or ideological objectives. (Joint Pub 1-02)

**Terrorist Incident Response Measures—**A set of procedures in place for response forces to deal with the effects of a terrorist incident.

**Threat and Vulnerability Assessment (VA)—**In antiterrorism, the pairing of a facility's threat analysis

and vulnerability analysis. (Joint Pub 1-02)

**Threat Working Group (TWG) —**TWGs are an AT/FP advisory body for the commander. Key functions include analyzing threats and providing recommendations to command concerning potential FPCON changes, AT and other measures based upon potential threats to facilities or personnel. Core membership, should include at a minimum, the ATO, AFOSI, Intelligence Office, Medical Intelligence Officer, Chief of Security Forces and other agencies as required by the installation commander.

**Vulnerability—**(1) The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. (2) The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment. (3) In information operations, a weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information systems.

**Vulnerability Assessment—**A Department of Defense, command, or unit-level evaluation (assessment) to determine the vulnerability of a terrorist attack against an installation, unit, exercise, port, ship, residence, facility, or other site. Identifies areas of improvement to withstand, mitigate, or deter acts of violence or terrorism.

**Weapons Of Mass Destruction (WMD)—**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. Weapons of mass destruction can be high explosives or nuclear, biological, chemical, and radiological weapons, but exclude the means of transporting or propelling the weapon where such means is a separable and divisible part of the weapon.

## Attachment 2

## REFERENCES TO DOD O-2000.12-H

**Table A2.1. At Standards and Associated Chapters/Appendices from DoD O-2000.12-H.**

| DOD Standard | Chapter and Number | Related Appendices |
|---|---|---|
| 1. DoD AT Policy | Chapter 1 | See also Ref (a) |
| 2. Development of CINC and/or Service and/or DoD Agency AT Program standards | Chapter 2 | |
| 3. Assignment of AT Operational Responsibility | Chapter 2 | See also Ref (a) |
| 4. AT Coordination in Overseas Locations | Chapter 12-14 | |
| 5. Comprehensive AT Program Development, Implementation, and Assessment | Chapter 4-13, 15-16 | 2, 4, 8, 10 |
| 6. Antiterrorism Officers (ATOs) shall be assigned, in writing, at each installation or base, and deploying organization (i.e., battalion, squadron, ship) | Chapter 15 | |
| 7. Application of DoD Terrorist Threat Analysis Methodology | Chapter 5 | 4 |
| 8. Threat Information Collection and Analysis | Chapter 5 | 2, 4, 8, 9, 10 |
| 9. Threat Information Flow | Chapter 5 | |
| 10. Potential Threat of Terrorist Use of Weapons of Mass Destruction | Chapter 20 | |
| 11. Adjustment of Force Protection Conditions (FPCONs) | Chapter 6 | 4 |
| 12. FPCON Measures Implementation | Chapter 6 | 4 |
| 13. FPCON Measures | Chapter 6 | 4, 11, 14, 15, 16 |
| 14. Commanders shall maintain a comprehensive AT Program for their areas of responsibility | Chapter 2 | 22, 23 |
| 15. Terrorism Threat Assessment | Chapter 17 | 2, 4, 8, 9, 10 |

| DOD Standard | Chapter and Number | Related Appendices |
|---|---|---|
| 16. AT Physical Security Measures | Chapter 7 | 2, 4, 22, 23 |
| 17. Terrorism Incident Response Measures | Chapter 17 | 4, 20, 22, 23 |
| 18. Terrorist Consequence Management Measures | Chapter 17 | 2 |
| 19. Training and Exercises | Chapter 20 | 2 |
| 20. AT Program Review | Chapter 2 | |
| 21. General Requirements for AT Training | Chapter 15 | |
| 22. Level I AT Awareness Training | Chapter 15 | |
| 23. AOR-Specific Training Requirements | Chapter 15 | |
| 24. Level II Antiterrorism Officer (ATO) Training | Chapter 15 | |
| 25. Training for High-Risk Personnel and High Risk Billets | Chapter 13, 15 | 6, 11, 14, 15, 16, 17 |
| 26. Vulnerability Assessments (VAs) of Installations | Chapter 9, 16 | |
| 27. Pre-deployment AT Vulnerability Assessment | Chapter 16, 19 | 19 |
| 28. Construction Considerations | Chapter 9 | 2 |
| 29. Facility and Site Evaluation and/or Selection Criteria | Chapter 10 | 2 |
| 30. AT Guidance for Off-Installation Housing | Chapter 11 | 2, 16, 17 |
| 31. Executive Protection and Protective Services | Chapter 13 | 14, 19 |

## Attachment 3

## FORCE PROTECTION CONDITIONS (FPCONS) AND MEASURES

A3.1. The FPCONs listed below describe progressive levels of terrorist threats to US military facilities and personnel. As DoD and Service's-approved terminology, these terms, definitions and security measures are intended to facilitate interservice coordination and support of US military antiterrorism and force protection activities. Selection of the appropriate response to terrorist threats remains the responsibility of the commander having jurisdiction or control over the threatened facilities or personnel. Commanders are responsible for ensuring measures tailored to their specific installation are developed commensurate with the appropriate FPCON level. A FPCON Individual Reference Card is available at **https://wwwmil.lackland.af.mil/afsf/**

**A3.2. FPCON NORMAL:** Commanders employ Random Antiterrorism Measures (RAMs) during this and all FPCONs to enhance force protection.

**A3.2.1. FPCON ALPHA:**

A3.2.1.1. Measure 1. At regular intervals, remind all personnel and family members 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.

A3.2.1.1.1. Based on the threat and intelligence sources, brief appropriate personnel on the threat.

A3.2.1.2. 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.

A3.2.1.3. Measure 3. Secure buildings, rooms and storage areas not in regular use.

A3.2.1.4. Measure 4. Increase security spot checks of vehicles and persons entering the installation and unclassified areas under the jurisdiction of the United States.

A3.2.1.5. Measure 5. Limit access points for vehicles and personnel commensurate with a reasonable flow of traffic.

A3.2.1.6. Measure 6. As a deterrent, apply measures 14, 15, 17 or 18 from FPCON BRAVO either individually or in combination with each other.

A3.2.1.7. Measure 7. Review all plans (to include AT, Disaster Preparedness Operations Plan 32-1 (or equivalent), Physical Security, and Medical Response/Mass Casualty Plans), most recent VA Report, orders, personnel details and logistics requirements related to the introduction of higher FPCONs.

A3.2.1.8. Measure 8. Review and implement security measures for high-risk personnel, facilities and critical infrastructure, as appropriate.

A3.2.1.9. 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 updated as necessary.

A3.2.1.10. Measure 10. Review plans and procedures and train facility occupants on individual protective actions for response to a WMD incident that occurs inside or outside of a facility.

A3.2.1.11. Measure 10A. Review mutual aid and host-tenant support agreements, memoranda of understanding, and host-nation memoranda of agreement to determine the level of WMD incident support the installation provides or receives and review support request and approval procedures. Update plans and checklists as needed.

A3.2.1.12. Measure 10B. Provide the base populace with both general and threat-specific information and protective actions through the installation Disaster Preparedness Information Program.

A3.2.1.13. Measure 10C. Secure all access to heating, ventilation, and air conditioning (HVAC) Mechanical Rooms. Lock and control the access to all interior and exterior doors that contain HVAC equipment.

A3.2.1.14. Measure 10D. Secure all access to hazardous and flammable material storage areas, especially storage areas where bulk quantities of hazardous or flammable materials are stored.

A3.2.1.15. Measure 10E. Take action to bring specialized disaster preparedness teams, hazardous material emergency response teams, and the Disaster Control Group (primary and alternate positions) to 100 percent of their authorized strength. Ensure personnel have been trained on local WMD attack response actions for 100 percent of currently assigned team members.

**A3.3. FPCON BRAVO:**

A3.3.1. Measure 11. Continue, or introduce, all measures listed in FPCONs 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 FPCONs.

A3.3.4. Measure 14. Move cars and objects; i.e., 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 explosives or biological agents.

A3.3.8. Measure 18. Check all deliveries to dining facilities, clubs, etc. Advise family members to check home deliveries.

A3.3.9. Measure 19. Increase security patrols and consider countersurveillance of military family housing, schools, dining facilities, clubs, child development centers and other soft targets to improve deterrence and defense and to build confidence among staff and family members.

A3.3.10. Measure 20. Make staff and family members 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, facilities and critical infrastructure, 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. Measure 28. CONUS installations will review NORAD Instruction 10-22, Nuclear, Biological, and Chemical Warning and Reporting System. OCONUS units will review their theater or MAJCOM guidance.

**A3.4. FPCON CHARLIE:**

A3.4.1. Measure 30. Continue, or introduce, all measures listed in FPCONs 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 and critical infrastructure.

A3.4.6. Measure 35. Issue weapons and individual protective equipment 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 at 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. Consider aircraft dispersal, or the dispersal of other high value mobile or relocatable assets, based on assessment of local threat from standoff weapons, vulnerability of the assets and operational feasibility.

A3.4.12. Measure 40A. Inspect and maintain WMD incident first responder equipment and supplies at the highest state of readiness and ready for immediate use. Identify local vendors that are able to provide rapid stocks of emergency response equipment and supplies.

A3.4.13. Measure 40B. Civil Engineer units will request their servicing weather unit to provide 12-hour and/or 24-hour effective downwind messages and chemical downwind messages.

**A3.5. FPCON DELTA:**

A3.5.1. Measure 41. Continue, or introduce, all measures listed for FPCON 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 buildings, critical infrastructure and 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 LEVELS

A4.1. The purpose of this attachment is to 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 four-step scale to describe the severity of the threat. These threat levels are established by DIA and the geographic CINCs and only apply to assessments of the terrorist threat to DoD interests. The following lists the threat levels and the combinations of analysis-based factors used to determine the level:

**A4.2.1. HIGH.** Anti-US terrorists are operationally active and uses large casualty producing attacks (WMD) as their preferred method of operation. There is a substantial DoD presence and the operating environment favors the terrorist.

**A4.2.2. SIGNIFICANT:** Anti-US terrorists are present and attack personnel as their preferred method of operation or a group uses large casualty producing attacks (WMD) as their preferred method but has limited operational activity. The operating environment is neutral.

**A4.2.3. MODERATE:** Terrorists are present but there are no indications of anti-US activity. The operating environment favors the Host Nation/US.

**A4.2.4. LOW:** No group is detected or the group activity is non-threatening.

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

**A4.3.1. OPERATIONAL CAPABILITY.** This factor focuses on the attack methods used by the group and other measures that enhance its effectiveness, such as state sponsorship and ingenious use of technology. The key element is whether the group has the capability and willingness to conduct large casualty producing attacks, for example a suicide vehicle bomb containing thousand of kilograms of explosives or WMD timed to kill the most personnel at the target. Groups that selectively assassinate individuals or conduct late night bombings causing limited property damage pose a decreasing threat. The ability to operate on a regional or transnational basis and the overall professionalism of the group is also assessed.

**A4.3.2. INTENTIONS.** This factor is the stated desire or history of terrorist attacks against US interests. Recent substantial attacks in the country or, if the group is transnational, the conduct of operations in other countries is the higher end of the threat scale. This is especially true if the intentions are anti-DoD. The basis of the group ideology, whether the group is more focused on the host nation rather than US interests is the other key component. Whether the group will react to high profile US led international events, such as intervention in the Balkans, is also considered and rated.

**A4.3.3. ACTIVITY.** This factor is an assessment of the actions the group is conducting and whether that activity is focused on serious preparations for an attack. The highest threat is credible indications of US targeting to include the movement of key operatives, final intelligence collection and movement of weapons to the target vicinity. Less threatening actions are contingency planning, training, and logistical support. Activities that would make the group less likely to attack, such as robust fund

raising or effective safe haven are considered. Whether the group has recently been disrupted by arrests or strikes on training camps will reduce the threat, at least in the short term.

**A4.3.4. OPERATING ENVIRONMENT.** This factor rates how the overall environment influences the ability, opportunity and motivation to attack DoD interests in a given location. An important element of this factor is the capability of the host nation security apparatus to combat terrorism, its degree of cooperation with the US and the quality of the reporting on terrorist groups in the country. A key element is whether there is a DoD presence and if so the type, size, location, political sensitivity and if temporary, its duration. It is also important to consider if the group is focused on DoD as its primary target for anti-US attacks. Another part of this factor is the overall political, economic and military stability of the country and its effect on the ability of a group to attack.

A4.4. DIA and the responsible geographic CINC 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. **A4.5.** Threat assessments provide information to assist commanders in determining the appropriate FPCONs. FPCON declarations remain the exclusive responsibility of commanders. Threat levels are not tied to FPCONs in any way, and should not be confused. National-level DoD organizations cannot provide all intelligence that might be needed to make FPCONs determinations. Information from regional and tactical intelligence, and local law enforcement authorities must also be considered.

A4.5. Threat assessments are not to be confused with DoD-designated high physical threat countries. DoD-designated high physical threat countries pertain exclusively to the DoD Travel Security Policy.

## Attachment 5

## AOR-SPECIFIC TRAINING

The following links are provided for commanders, installation ATOs, and others conducting Level I Antiterrorism Training. These sites are to be used to get the area of responsibility (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.

**US CENTRAL COMMAND (CENTCOM)**

CLASSIFIED: Ccj2_intel-s.centcom.smil.mil/jic/terrorism/summary/indextmp.htm

UNCLASSIFIED: **http://www.centcom.mil**

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

**US SOUTHERN COMMAND (SOUTHCOM)**

CLASSIFIED: 164.232.22.173

UNCLASSIFIED: Foreign Clearance Guide and the State Department Travel Advisory Page at **http://travel.state.gov/travel_warnings.html**

**US EUROPEAN COMMAND (EUCOM)**

CLASSIFIED: **http://www.eucom.smil.mil/ecsm**

UNCLASSIFIED: **http://www.eucom.mil/hq/ecsm**

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

**US JOINT FORCES (JFCOM)**

CLASSIFIED: 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

**US PACIFIC COMMAND (PACOM)**

CLASSIFIED: **http://www.hq.pacom.smil.mil**

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

UNCLASSIFIED: **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: **http://nmcc20a.nmcc.smil.mil/~dj3cleap/j34.html**

Unclassified CINC Homepages can be accessed via the DoD Antiterrorism Homepage at: **http://www.dtic.mil/jcs/force protection**

Prior to travel, all service members and family members traveling to a geographic CINC's AOR are advised to consult the Foreign Clearance Guide and the State Department Travel Advisory Homepage at **http://travel.state.gov/travel_warnings.html**.

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

## Attachment 6

## INFORMATION AND PROCEDURES FOR INSTALLATIONS RECEIVING AIR FORCE SECURITY FORCES CENTER AT/FP VULNERABILITY ASSESSMENTS

A6.1. Vulnerability assessments assist installation commanders in meeting their AT responsibilities and should be viewed as a commander's tool to identify vulnerabilities and options (procedural and technical) to reduce the potential impact of terrorist attacks. The focus of VAs is on the protection of Department of Defense (DoD) personnel and their family members. To best support the installation commander, close coordination between the Vulnerability Assessment Team (VAT) and the commander's staff is necessary. Prior to the VAT's arrival, a message detailing the VAT''s requirements will be sent to the unit being assessed.

A6.2. The following items need to be provided to the VAT prior to their arrival:

A6.2.1. A copy of the installation terrorism threat assessment, as required by para **2.15.** of this instruction.

A6.2.2. A brief, unclassified overview of the installation units and mission(s) to include number of personnel assigned.

A6.2.3. Ten copies of a prioritized list of buildings, facilities and/or specific AT concerns, which the installation commander may ask the VAT to focus on. When constructing the list, remember the primary focus of the VAT is protection of personnel and secondary considerations are priority resources. The buildings and facilities typically listed are those with high occupancy or US Government symbolic representation.

A6.2.4. An installation organization chart with a list of tenant units.

A6.2.5. An installation telephone book.

A6.2.6. A copy of existing AT plans and related plans (i.e., installation security plans, resource protection plans, force protection plans to include FPCON procedures [mail FPCON material separately or you may have to use procedures for mailing classified documents], emergency preparedness plans, mass casualty response plans, terrorist incident response plans, emergency action plans, medical contingency response plans, OPLANs 10-2, Base Civil Engineer (BCE) contingency plans, CE general plans, water VAs, infrastructure VAs, etc.).

A6.2.7. Ten copies of the installation map of the type normally provided to newcomers.

A6.2.8. Two copies of the installation map from the base comprehensive plan; tab C-1 (scale 1 inch = 400 feet, full size sheets).

A6.2.9. Installation MILCON and O&M facility project listings for current year and all out years.

A6.2.10. The installation commander's full name and official mailing address for receiving classified information.

A6.2.11. List of average populations in higher occupancy buildings (dorms, dining facilities, HQ, community centers, etc.) and any other installation sites or activities that produce a high population (formation, sports events, ceremonies, open houses, etc.).

A6.2.12. Assistance with lodging arrangements. Please make reservations for 10 personnel (maintaining team integrity is requested). Please also provide the name, address, telephone numbers and confirmation numbers (if available) for lodging.

A6.2.13. Location and telephone numbers of the proposed VAT work center.

A6.2.14. An emergency contact telephone number to notify the installation if the VAT is delayed enroute.

A6.2.15. The name and location of the nearest commercial airport and a map to assist the VAT with traveling from the airport to the installation.

A6.2.16. List of points of contact (POCs) from the following areas: AT Officer/NCO, Security Forces Operations, Physical Security and Planning, AFOSI, CE Engineering Flight, Operations Flight, Readiness Flight, EOD, Fire Department, Medical Services (Public Health, Bioenvironmental Engineering, mass casualty and triage), Communications, Public Affairs, Command Post, Intelligence and Staff Judge Advocate (SJA). Please provide the name, rank and contact number for each POC.

A6.2.17. Copies of previous AT assessments.

A6.3. The following information should be made available to the VAT upon their arrival/during the course of the assessment:

A6.3.1. Access to the CE unit's drawing vault.

A6.3.2. Information on security measures to include: manning (armed guards, shift staffing, etc.), alarm/sensor descriptions, defensive mechanisms (charged fences, etc.), major equipment items (vehicles, radios, weapons, personal protective equipment, etc.) and jurisdiction maps and documents.

A6.3.3. Cooperative agreements or memorandums of understanding with local authorities in the following areas: law enforcement, medical and fire services.

A6.3.4. Information on the installation's fire department including a list of equipment, manpower (number and position) and volume of available fire fighting agent.

A6.3.5. A list of surrounding area hospitals and their capabilities.

A6.3.6. A list of surrounding area fire departments and their capabilities.

A6.3.7. Information on the installation's power systems including an electrical distribution site plan, locations of substations, a list of emergency generators with location, size, fuel, etc., and a list of critical uninterruptible power systems.

A6.3.8. Information on the installation's water systems including a water distribution site plan with wells, reservoirs, treatment facilities and other storage locations.

A6.3.9. Information on the installation's natural gas distribution system.

A6.3.10. Information on the installation's petroleum, oil, and lubrication (POL) distribution system.

A6.4. The VAT requires the following administrative/logistical support during the course of the assessment:

A6.4.1. Use of a work center. Ideally, the work center (conference room, training room, office space, etc.) should have sufficient space and furniture to accommodate approximately 10 team members with

laptop computers and printers, wall and table space to display maps and engineering diagrams, and access to at least two class A telephones plus two separate class a analog lines for computer modems. The team will bring most of their own office supplies, but will need paper and possibly some other minor items.

A6.4.2. Access to a shredder for destruction of classified information.

A6.4.3. Access to a fax.

A6.4.4. Access to a photocopier.

A6.4.5. Access upon arrival and during the assessment to a container to store classified information. The VAT travels with classified information and will need classified storage capability beginning on the day of arrival and every day up to and including the day of departure.

A6.4.6. Coordination of vehicle passes, if required. The VAT will obtain and use approximately four rental vehicles during the assessment.

A6.4.7. Coordination of any required security arrangements to include badges allowing access to all areas of the installation and letters for permission to photograph, if required. If the VAT will be restricted from certain areas of the installation, please inform the VAT POC.

## Attachment 7

## LEVEL II AT/FP TRAINING SCHOOLS FOR AT OFFICERS/NCOS

There are numerous multiservice schools conducting Level II AT training. Attending any of the following schools may certify USAF personnel:

### United States Air Force

Air Combat Command Ground Training Squadron
Nellis AFB, NV
Phone: DSN 682-4889

Air Mobility Warfare Center
McGuire AFB, NJ
Phone: DSN 944-4101 (ext 185)

Air Force Special Operations Command
Hurlburt Field, FL
Phone: DSN 579-6330

Air Force Reserve Command
610th Security Forces Squadron
Naval AS, Ft Worth TX
Phone: DSN 739-5101 (ext 141, 134, 127)

US Air Forces in Europe Creek Defender
Sembach AB, GE
Phone: DSN (314) 496-7403

### United States Army

Force Protection Unit Advisor Course, U.S. Army MP School
Fort Leonard Wood, MO
Phone: DSN 581-2061

West Virginia Army National Guard
Charleston, WV
Phone: DSN 623-6413

National Interagency Civil-Military Institute (NICI)
San Luis Obispo, CA
Phone: DSN 630-6774/Comm 1-800-926-5637

US Army MP School Mobile Training Team
Phone: DSN 581-2061

Eighth U.S. Army AT/FP Level II Course
Phone: DSN (315) 724-6021

FORSCOM MTTs
Phone: DSN 367-6871

## United States Navy

Naval Criminal Investigative Service (NCIS) MTT Atlantic
Little Creek, VA
Phone: DSN 253-8925

NCIS MTT Pacific
San Diego, CA
Phone: DSN 735-8934

Expeditionary Warfare Training Group Atlantic
Naval Amphibious Base, Little Creek, VA
Phone: DSN 253-7293

Fleet Training Center
San Diego, CA
Phone: DSN 526-7759

# Attachment 8

## ANTITERRORISM RESOURCE ALLOCATION TEMPLATE

CLASSIFICATION

Appendix A

CINC POM FY 03-07

AT/FP Requirements Worksheet

POC:

Phone:

E-mail:

| Control # (a) | Service/ Agency (b) | Com - ponent (c) | Location FPCON (d) | Priority (e) | Req'ts Title (f) | Req'ts Description (g) | Type IVA/ Date (h) | Threat (H-S-M-L) (i) | Vulnerability (j) | Asset Criticality (k) | AT Plan Effectiveness (H-M-L) (l) | Cmdrs Risk Assessment - Impact If Not Funded (H-M-L) (m) | TAB O Category (n) | IPL (o) | Appropriation (p) | FY03 (q) | FY04 (r) | FY05 (s) | FY06 (t) | FY07 (u) | Total FY03-07 ($M) (v) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| E-AF-0001-00 | AF | USAFE | TBD AB ALPHA | M | CCTV for transitory dormitory | Dormitory located close to base perimeter and near civilian roadway. Insufficient standoff distance and no method to provide occupants or security forces with early warning in event of IED detonation or other incidents. | JSIVA Provide the date and specific page and paragraph reference for the write up. | M Threat Information provided by EUCOM | H No control over local roadway, dorm in close proximity of the base perimeter, no early warning mechanism in place. | H Houses personnel essential to successful air operations. | H Based on size of staff, whether full or part time, status of plans etc... | H Local Base Commander's rating Explain why/rationale to support his rating. | PSE | Y | 3400 (O&M) | 0.400 | | | | | 0.400 |
| | | | | | | | | | | | | | | | 3600 (Mil Pers) | | | | | | 0.000 |
| | | | | | | | | | | | | | | | 3600 (RDT&E) | | | | | | 0.000 |
| | | | | | | | | | | | | | | | 3080 (Procurement) | | | | | | 0.000 |
| E-AF-0002-00 | AF | USAFE | TBD AB M | M | Contractor Logistic Support Tactical Automated Security | Procurement of this system was based on the MAJCOM providing for the sustainment of the equipment. Without this funding the equipment will not be available to provide early warning against possible attacks. | USAFE VAT Provide the date and specific page and paragraph reference for the write up. | M-H Threat information provided by EUCOM. System employed Theater-wide | M Sensor suite requires maintenance to maintain optimal performance, without which detection capability is significantly degradated. | H System employed to protect people and assets at deployed and fixed sites to enhance detection probability and mission accomplishment | M Command wide assessment of AT/FP office and program based on informaiton outlined above. | H The sustainment of this system is critical to our overall force protection program. Without this equipment early detection of threats in our areas of operations is impossible. | PSE | Y | 3400 (O&M) | 0.300 | 0.300 | 0.300 | 0.300 | 0.300 | 1.500 |
| | | | | | | | | | | | | | | | 3600 (Mil Pers) | | | | | | 0.000 |
| | | | | | | | | | | | | | | | 3600 (RDT&E) | | | | | | 0.000 |
| | | | | | | | | | | | | | | | 3080 (Procurement) | | | | | | 0.000 |
| E-AF-0003-00 | AF | USAFE | TBD AB ALPHA | M | DODDS Contract Guards | The DODD Schools located off installation and not patrolled by base security forces require on-site security guard presence to deter possible hostile activity. | JSIVA Provide the date and specific page and paragraph reference for the write up. | M | H Schools located in host nation and not under protection of the US forces, facility is not fenced, or patrolled and is easily recognizable | H Significant Quality of Life issue for assigned personnel with school aged children. | M Command wide assessment of AT/FP office and program based on informaiton outlined above. | L Rated lower by the Commander because the deficiency does not become an issue until FY06-07. Commander agrees that it is important to provide the protection. | PSE | Y | 3400 (O&M) | | | | 0.700 | 0.700 | 1.400 |
| | | | | | | | | | | | | | | | 3600 (Mil Pers) | | | | | | 0.000 |
| | | | | | | | | | | | | | | | 3600 (RDT&E) | | | | | | 0.000 |
| | | | | | | | | | | | | | | | 3080 (Procurement) | | | | | | 0.000 |
| E-AF-0004-00 | AF | USAFE | TBD AB ALPHA | M | AT/FP Manpower | The tasks associated with running a viable AT/FP program cannot be done in a timely manner without dedicated personnel to manage the execution of the program at the installation level. Also need the associated O&M funding. | JSIVA Provide the date and specific page and paragraph reference for the write up. | M-H Threat information provided by EUCOM. System employed Theater-wide | M-H Based on the known location of our installations and the missions that are performed. | H Personnel assigned to these locations are responsible for meeting mission requirements. Without them we can't get it done. | L-M Overall Command assessment of the status of our program. Because of the lack of full time folks to make it happen. | H I cannot do more with less. If we're serious about protecting the force then we have to dedicate the resources and personnel to get the job done right the first time. | SFT | Y | 3400 (O&M) | 0.316 | 0.315 | 0.315 | 0.315 | 0.315 | 1.575 |
| | | | | | | | | | | | | | | | 3600 (Mil Pers) | 0.895 | 1.085 | 1.085 | 1.085 | 1.385 | 5.525 |
| | | | | | | | | | | | | | | | 3600 (RDT&E) | | | | | | 0.000 |
| | | | | | | | | | | | | | | | 3080 (Procurement) | | | | | | 0.000 |
| E-AF-0005-00 | AF | USAFE | TBD AB ALPHA | M | Install Perimeter Lighting | Provide the ability to see personnel or vehicles approaching before they pose a threat to the base population. Will allow security forces to identify possible threats and respond to them at a longer distance from their intended target. | JSIVA Provide the date and specific page and paragraph reference for the write up. | M Threat information provided by EUCOM. | H No current capability to detect personnel or vehicles outside the base perimeter. During the hours of darkness | H Base houses personnel and critical infastructure essential to successful air operations. | M Command wide assessment of AT/FP office and program based on informaiton outlined above. | M This project would enhance our ability to detect and intercept personnel attempting to gain unauthorized access to the installation. | SI | Y | 3400 (O&M) | 0.017 | | | | | 0.017 |
| | | | | | | | | | | | | | | | 3600 (Mil Pers) | | | | | | 0.000 |
| | | | | | | | | | | | | | | | 3600 (RDT&E) | | | | | | 0.000 |
| | | | | | | | | | | | | | | | 3080 (Procurement) | | | | | | 0.000 |
| E-AF-0006-00 | AF | USAFE | TBD AB ALPHA | M | Up-Armored High Mobility Multipurpose Wheeled Vehicles (UA-HMMWV) | New requirement levied by NATO for responding security force tp be protected by armored vehicles. Their role is to provide protection for critical mission assets and recapture those assets should they be seized by unauthorized personnel. Responding for | USAFE VAT Provide the date and specific page and paragraph reference for the write up. | M-H Threat information provided by EUCOM. | H Security Forces have no current hardened vehicles to meet this requirement. They would be exposed to hostile fire while attempting to respond to an incident. | H These resouces are absolutely critical to national security and must be afforded the best possible protection available. | H-L Command wide assessment of AT/FP office and program based on informaiton outlined above. | M These vehicles would ensure the safety of responding security forces. Without them we could lose assets and personnel and damage eur national security posture. | PSE | Y | 3400 (O&M) | | | | | | 0.000 |
| | | | | | | | | | | | | | | | 3600 (Mil Pers) | | | | | | 0.000 |
| | | | | | | | | | | | | | | | 3600 (RDT&E) | | | | | | 0.000 |
| | | | | | | | | | | | | | | | 3080 (Procurement) | 1.600 | 1.700 | 1.800 | 3.900 | 4.500 | 13.500 |

Date: