BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 10-245

21 SEPTEMBER 2012

30TH SPACE WING
Supplement
28 MARCH 2013
Certified Current, 30 March 2017
Operations

ANTITERRORISM (AT)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **http://www.e-Publishing.af.mil** for downloading or ordering

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: AF/A7S

Certified by: AF/A7S
(Brig Gen Allen J. Jamerson)

Pages: 96

Supersedes: AFI 10-245, 30 March 2009

(30SW)

OPR: 30 SW/CCH

Certified by: 30 SW/CV

Pages:9

This instruction implements Air Force Policy Directive (AFPD) 10-2, *Readiness,* and Department of Defense Instruction (DoDI) 2000.16, *DoD Antiterrorism (AT) Standards.* It is consistent with directions in Department of Defense Instruction (DoDI) 2000.12, *DoD Antiterrorism (AT) Program*; Department of Defense (DoD) O-2000.12-H, *DoD Antiterrorism Handbook*; DoDI 6055.17, *DoD Installation Emergency Management (IEM) Program*; AFDD 4-0, *Combat Support*; AFDD 3-10, *Force Protection*; AFPD 31-1, *Integrated Defense*; AFPD 10-25, *Emergency Management*; AFPD 10-26, *Counter-Chemical, Biological, Radiological, and Nuclear Operations*; and AFPD 10-39, *Safeguarding Biological Select Agents and Toxins*. It establishes responsibilities and guidance for the Air Force (AF) Antiterrorism (AT) Program. This Air Force Instruction (AFI) applies to all military and civilian Air Force personnel, Air Force Reserve Command and Air National Guard units and other individuals or organizations as required by binding agreement or obligation with the Department of the Air Force. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) Air Force Manual (AFMAN) 33-363, *Management of Records,* and

disposed of IAW the Air Force Records Disposition Schedule (RDS) located at **https://www.my.af.mil/afrims/afrims/afrims/rims.cfm**. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, Recommendation for Change of Publication; route AF Form 847s from the field through the appropriate functional chain of command.

(30SW) AFI 10-245 dated 21 September 2012 is supplemented as follows. This supplement prescribes the use of 30th Space Wing (30 SW) AT Visual Aids (VA) necessary for the protection of personnel, property, and resources. This supplement applies to all 30 SW units, subordinates, and agencies assigned to Vandenberg AFB (VAFB) including contractors, and visiting personnel. This publication may be supplemented at any level, but all supplements must be routed to the Office of Primary Responsibility (OPR) listed above for coordination prior to certification and approval. Refer recommended changes and questions about this publication to the OPR listed above using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate chain of command. Requests for waivers must be submitted to the OPR listed above for consideration and approval. This publication requires the collection and or maintenance of information protected by the Privacy Act of 1974 authorized by Title 10, U.S.C 8013, Secretary of the Air Force and E.O. 9397, as amended. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

SUMMARY OF CHANGES

This document is substantially revised and must be completely reviewed. Throughout the document, the AT Program has been integrated with Integrated Defense (ID), Emergency Management (EM), and Critical Asset Risk Management (CARM) programs to support Force Protection (FP). In addition, AF functional roles and responsibilities have been updated; requirements for AT Training have been revised; and several FPCON measures have been revised or updated. Attachment 6—The Antiterrorism Deviation Program has been added to establish new AF deviation procedures for AT construction standards, and Attachment 7—Categories of Suspicious Behavior has been added to supplement guidance on eGuardian.

Chapter 1—AIR FORCE ANTITERRORISM PROGRAM **6**

1.1. Air Force Antiterrorism Program. 6

1.2. AT Responsibility. 6

1.3. AF AT Program Policy. 7

1.4. AT Program Roles and Responsibilities. 8

Chapter 2—ANTITERRORISM STANDARDS **19**

2.1. Standard 1: 19

	2.2.	Standard 2:	19
	2.3.	Standard 3:	20
Figure	2.1.	AT Risk Management Process	21
	2.4.	Standard 4:	21
	2.5.	Standard 5:	22
	2.6.	Standard 6:	22
	2.7.	Standard 7:	26
Table	2.1.	AT Threat Planning Scenarios	26
	2.8.	Standard 8:	28
	2.9.	Standard 9:	29
	2.10.	Standard 10:	32
	2.11.	Standard 11:	32
	2.12.	Standard 12:	33
	2.13.	Standard 13:	33
	2.14.	Standard 14:	34
	2.15.	Standard 15:	35
	2.16.	Standard 16:	36
	2.17.	Standard 17:	37
	2.18.	Standard 18:	37
	2.19.	Standard 19:	38
	2.20.	Standard 20:	38
	2.21.	Standard 21:	39
	2.22.	Standard 22:	40
	2.23.	Standard 23:	41
	2.24.	Standard 24:	41
	2.25.	Standard 25:	42
Table	2.2.	Level I - AT Awareness Training Requirements	44
	2.26.	Standard 26:	44
Table	2.3.	Level II – ATO and ATR Training Requirements	46
	2.27.	Standard 27:	46
Table	2.4.	Level III - Pre-Command AT Training Requirements	47
	2.28.	Standard 28:	47
	2.29.	Standard 29:	48

2.30. Standard 30: 48
2.31. Standard 31: 49
2.32. Standard 32: 50

Chapter 3—(Added-30SW) DESCRIPTION OF 30 SW VISUAL AIDS (VA) 51

3.1. (Added-30SW) All 30 SW FPCON VAs 51
3.2. (Added-30SW) The 30 SW FPCON VA signs- 51
3.3. (Added-30SW) The 30 SW/CCH 51

Chapter 4—(Added-30SW) GENERAL GUIDANCE FOR THE USE OF 30 SWVA 10-1 THROUGH 30 SWVA 10-5A, FPCON SIGNS 52

4.1. (Added-30SW) The proper 30 SW FPCON VA sign- s 52
4.2. (Added-30SW) All facilities- 52
4.3. (Added-30SW) Consider storing FPCON signs in a holder adjacent to doors. 52

Chapter 5—(Added-30SW) USE OF THE 30 SWVA 10-1 THROUGH 30 SWVA 10-5, FPCON SIGNS 53

5.1. (Added-30SW) Use of the FPCON Normal Real-World Visual Aid, 30 SWVA 10-5: 53
5.2. (Added-30SW) Use of the FPCON Alpha Real-World Visual Aid, 30 SWVA 10-1: 53
5.3. (Added-30SW) Use of the FPCON Alpha Exercise Visual Aid, 30 SWVA 10-1A: 53
5.4. (Added-30SW) Use of the FPCON Bravo Real-World Visual Aid, 30 SWVA 10-2: 53
5.5. (Added-30SW) Use of the FPCON Bravo Exercise Visual Aid, 30 SWVA 10-2A: 53
5.6. (Added-30SW) Use of the FPCON Charlie Real-World Visual Aid, 30 SWVA 10-3: 53
5.7. (Added-30SW) Use of the FPCON Charlie Exercise Visual Aid, 30 SWVA 10-3A: 53
5.8. (Added-30SW) Use of the FPCON Delta Real-World Visual Aid, 30 SWVA 10-4: 53
5.9. (Added-30SW) Use of the FPCON Delta Exercise Visual Aid, 30 SWVA 10-4A: 53

Chapter 6—(Added-30SW) USE OF 30 SWVA 10-6 THROUGH 30 SWVA 10-9, ANTITERRORISM VISUAL AIDS 54

6.1. (Added-30SW) Four additional 30 SW AT VAs are available. 54

6.2. (Added-30SW) Use of the Antiterrorism Memory Jogger Card, 30 SWVA 10-6: 54

6.3. (Added-30SW) Use of the Suspicious Package/Letter/Unattended items Visual Aid, 30 SWVA 10-7: 54

6.4. (Added-30SW) Use of the Suspicious Powder or Substance Visual Aid, 30 SWVA 10-8: 54

6.5. (Added-30SW) Use of the Bomb Threats Visual Aid, 30 SWVA 10-9: 54

Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 55

Attachment 1—(30SW) GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 71

Attachment 2—FORCE PROTECTION CONDITION (FPCON) MEASURES 72

Attachment 3—TERRORIST THREAT LEVELS 82

Attachment 4—RISK MANAGEMENT AND RESOURCING PROCESSES 84

Attachment 5—AF APPROVED LEVEL II - ATO CERTIFICATION TRAINING COURSES 86

Attachment 6—THE ANTITERRORISM STANDARDS FOR BUILDINGS DEVIATION PROGRAM 87

Attachment 7—CATEGORIES OF SUSPICIOUS ACTIVITY 90

Attachment 8—(Added-30SW) VISUAL AIDS 92

Chapter 1

AIR FORCE ANTITERRORISM PROGRAM

1.1. Air Force Antiterrorism Program. This instruction establishes guidance and procedures for the Air Force Antiterrorism Program and supports the Department of Defense AT Program. The AT Program is a high priority, comprehensive program which focuses on defensive measures to reduce the risk to AF personnel and property to terrorist acts. The guidance and procedures for AT risk management provide guidance on collecting and disseminating timely terrorist threat information, guide development and support the implementation of comprehensive AT plans, ensure AT training and exercises for all AF members, provide guidance for allocation and application of AT resources, and establish procedures for comprehensive AT program reviews.

1.2. AT Responsibility. AT is a command responsibility which must be thoroughly integrated into every unit mission. Commanders and equivalents at all levels have the responsibility and authority to enforce appropriate AT standards and measures. Commanders and equivalents must be aware of evolving threats against their command and continually review their AT posture using the Integrated Defense Risk Management Process (IDRMP), to manage risk and appropriately adjust the posture of elements and personnel subject to their control. The next level up the chain of command must be notified and mitigate or accept any AT risk that cannot be controlled to an acceptable level within a commander's resources.

1.2.1. The Major Command (MAJCOM) AT Program Manager (ATPM), the Numbered Air Force (NAF) Antiterrorism Officer (ATO), the Installation ATO, and the Unit Antiterrorism Representative (ATR) are advisors to commanders at each respective level. They shall not assume AT responsibility but are charged with advising the commander or equivalent on AT issues, managing the AT Program, and coordinating implementation of the AT Program.

1.2.2. The AF Antiterrorism program is a cross-functional supported program which utilizes the skills and expertise of a variety of AF professionals. MAJCOM and Installation Commanders will identify personnel on their staff to oversee the antiterrorism program and act as the subject matter expert responsible for executing both DoD and AF-directed AT requirements across a major command or installation, and coordinates the efforts of key functional areas to ensure synergy on behalf of the commander. At a minimum, Security Forces, Air Force Office of Special Investigations (AFOSI), Intelligence, Civil Engineers (to include Emergency Management, Engineering Explosive Ordnance Disposal (EOD) and Fire Emergency Services), Force Support, Command Post, Public Affairs, Communications, Contracting, Operations, Public Health and Bioenvironmental Engineering (food and water), Judge Advocate, and Comptroller must coordinate efforts to achieve an effective AT posture. The installation ATO is responsible to coordinate among these key players and facilitate the integration and coordination of their efforts on behalf of the commander. As a sub-element of the overarching FP program, AT must be integrated with and complement other programs supporting FP.

1.2.3. Additionally, an effective AT program requires participation from every member of the force. Each individual must maintain awareness of potential terrorist threats, practice personal security measures, and report suspicious activity.

1.2.4. The AT Program shall be considered when establishing and exercising support agreements or mutual aid agreements (MAA) with local agencies, whether CONUS or OCONUS. At a minimum, agreements must establish procedures for information sharing, must address AT capabilities and limitations, and must outline roles and responsibilities during response to acts of terrorism. If agreements with outside agencies do not provide sufficient support to the AT program, associated vulnerabilities will be entered into Core Vulnerability Assessment Management Program (CVAMP) explaining the lack of support.

1.2.5. Installation AT planning shall include a communications plan to inform the base populace through Public Affairs of the need to report suspicious activities/incidents, the nature of items to be reported, and how to report them.

1.2.5.1. Eagle Eyes. The Eagle Eyes program is an Air Force AT initiative that enlists the eyes and ears of Air Force members, civilians, contractors, and dependants. The Eagle Eyes program will inform the community on how to recognize possible terrorist activity and how to report suspicious behavior. Armed with this information, all individuals can recognize elements of potential terror planning when they see it. The program provides a network of local, 24-hour phone numbers to call whenever a suspicious activity is observed. Each installation shall establish procedures to receive and log suspicious activity reports and suspicious incident reports (SAR/SIR) and to pass those reports expeditiously to their servicing AFOSI detachment for appropriate action. Eagle Eyes is an AFOSI-led program requiring close and continuous liaison and coordination between the installation Security Forces Squadron, AFOSI Detachment, Installation ATO, Command Post, Public Affairs office and others. This program implements the spirit and intent of DoDI 2000.26, *Suspicious Activity Reporting*. See Attachment 7 for the categories of suspicious activities that are required to be reported.

1.2.5.2. Security Forces Squadrons shall develop local procedures, in concert with their supporting AFOSI Detachment, to log and track SAR/SIR in order to expeditiously submit all reporting received from the public or other sources with a possible/potential linkage to terrorism using the eGuardian system. MAJCOM ATPM, Installation ATO, and Information Fusion Cell (IFC) will have "read" access to the eGuardian system. Categories of information to report via eGuardian are shown at Attachment 7 to this publication. AFOSI is the OPR for eGuardian and shall make any necessary entries to the system.

1.3. AF AT Program Policy. The AF AT Program supports and implements DoD policy as described in DoDI 2000.12, which establishes DoD policies and responsibilities for AT. AT standards and AF-specific guidance for implementing the AT Program will be established based on guidance in DoDI 2000.16.

1.3.1. Geographic Combatant Commander (GCC) AT Policy Precedence. IAW the Unified Command Plan (UCP) and DoDI 2000.12, GCC AT policies take precedence over the AT policies and programs of any other DoD Component operating or existing in the GCC area of responsibility (AOR) except for those under the security responsibility of a Chief of Mission (CoM), to include exercising tactical control (TACON) for FP. TACON for FP is in addition to a Combatant Commander's normal exercise of operational control (OPCON) over assigned forces. All DoD personnel traveling into a GCC's AOR shall familiarize themselves and comply with all AOR-specific AT policies. AF Components to GCCs bridge

gaps between GCC and AF policies. In the application of AT policy, the more restrictive guidance will be applied.

1.3.2. AT Policy Concerning Tenants and Privatized Support on AF Property. All tenant units, non-DoD tenants, DoD elements, and privatized support to AF property and activities shall be included in the AT Program, adhere to AT requirements, and participate in the host installation AT Program. Commanders shall ensure agreements are in place which specifically obligate compliance with the AT requirements in this AFI and with applicable portions of Unified Facilities Criteria (UFC) standards.

1.3.3. AT Policy Regarding Travel. All personnel (military, civilians, dependent family members, and contractors supporting DoD operations IAW contract provisions) shall comply with GCC, theater, country, and special clearance requirements (Electronic Department of Defense Foreign Clearance Guide, **https://www.fcg.pentagon.mil**/) prior to departing the continental United States (CONUS), traveling into another GCC's AOR, or traveling between countries outside the continental United States (OCONUS). AF personnel in-transit on Leave/Temporary Duty (TDY) or deployment orders shall also comply with AT Standard 29 of this AFI.

1.4. AT Program Roles and Responsibilities.

1.4.1. General. AF commanders at all levels (or equivalent civilian directors) assigned AT responsibility shall establish and maintain active AT programs IAW DoD, GCC, AF, and all other applicable AT guidance. All commanders have the authority and responsibility to enforce appropriate security measures to ensure the protection of DoD elements and personnel subject to their control while pursuing mission accomplishment and shall ensure the AT awareness and readiness of all DoD elements and personnel assigned or attached.

1.4.1.1. AF organizations/activities shall develop local guidance to implement this Instruction, such as MAJCOM or installation supplements/instructions/plans, that identify AT-specific operational responsibilities, to include the scope of AT responsibility for facilities and operations that do not meet the legal definition of an installation (e.g., recruiting offices and other geographically separated units [GSUs]).

1.4.1.2. AT activities shall support GCCs as they exercise overall responsibility for AT within their respective AORs. Commanders will ensure such activities and actions comply with applicable Intelligence Oversight rules, Status of Forces Agreements (SOFA) and the DoD Foreign Clearance Guide.

1.4.1.3. MAJCOMs, field operating agencies (FOA), direct reporting units (DRU), AF Components to the GCC, Component-NAFs (C-NAF), NAFs, Wings, Installations and separate facilities with commanders or equivalent civilian directors assigned AT responsibility shall have an active AT program tailored to the local security environment.

1.4.1.4. GSUs attached to an installation will be included in the AT Plan and comply with all installation AT program requirements. Installation ATOs shall ensure coordination on AT program elements and responsibilities regarding GSUs.

1.4.1.5. Intelligence supports FP with readiness training, mission planning, unit deployments and other mission execution functions, including, but not limited to, integrated defense support, critical asset risk management program, and emergency

management. Both OCONUS and CONUS, AFOSI conducts counterintelligence activities in support of AT. AFOSI works with foreign, federal, state, tribal and local law enforcement, security, intelligence and counterintelligence agencies to identify, exploit, and neutralize criminal, terrorist and foreign intelligence threats to the US Air Force, DoD, and US Government (USG).

1.4.2. Headquarters Air Force (HAF) Responsibilities:

1.4.2.1. Assistant Secretary of the Air Force, Financial Management and Comptroller (SAF/FM). SAF/FM shall:

1.4.2.1.1. Advise commanders, the HAF Force Protection Working Group (FPWG) and HAF Force Protection Steering Group (FPSG) on financial processes and procedures to effectively resource AT program requirements through planning, programming, budgeting and execution (PPB&E); and Combatant Commander's Initiative Fund (CCIF).

1.4.2.1.2. Provide long range financial planning for the AT Program.

1.4.2.2. Inspector General (SAF/IG). SAF/IG shall provide counterintelligence (CI) and criminal investigative support to the AT program through HQ AFOSI. Reference AFPD 71-1, *Criminal Investigations and Counterintelligence*.

1.4.2.3. Judge Advocate General of the Air Force (AF/JA). AF/JA shall provide legal advice on AT matters and shall be a primary member of the HAF FPWG and HAF FPSG to ensure all legal aspects are addressed during the mitigation process of vulnerabilities and other legal issues.

1.4.2.4. Director of Public Affairs (SAF/PA). SAF/PA shall:

1.4.2.4.1. Incorporate communication activities into the public affairs program in order to combat terrorism.

1.4.2.4.2. Ensure all terrorist incident/threat report releases to the media are coordinated with Office of the Assistant Secretary of Defense, Public Affairs (OASD)/PA prior to release.

1.4.2.4.3. After coordination with OASD/PA, SAF/PA may acknowledge increased security measures have been taken in response to a possible or real terrorist threat/incident. Requests for coverage of counter-terrorism forces will not be approved.

1.4.2.5. Surgeon General (AF/SG). AF/SG shall:

1.4.2.5.1. Serve as the OPR for Force Health Protection (FHP) and the Public Health Emergency Officer (PHEO) IAW AFI 10-2603, *Emergency Health Powers on Air Force Installations*.

1.4.2.5.2. Supervise food and water protection programs as outlined in AFI 10-246, *Food and Water Protection Program*. Coordinate food and water vulnerability assessments (VA) with AT VAs at all levels and ensure reports facilitate CVAMP format/entries.

1.4.2.6. Safety (AF/SE). AF/SE shall assist functional areas in ensuring safety is considered during AT planning and observed during AT operations.

1.4.2.7. Deputy Chief of Staff of the Air Force, Manpower, Personnel and Services (AF/A1). AF/A1 shall:

1.4.2.7.1. Provide AT guidance for personnel issues.

1.4.2.7.2. Provide specific policy and guidance for documenting pre-deployment AT training and special position or duty qualifications on deployment orders.

1.4.2.7.3. Ensure a system exists for tracking formal AT training IAW AT Standard 24, DODI 2000.16.

1.4.2.7.4. Notify AF/A7S when a deficiency is identified in manpower standards supporting appointed AT positions.

1.4.2.8. Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance (AF/A2). AF/A2 shall:

1.4.2.8.1. Provide policy for planning, programming, training, and budgeting resources necessary to ensure the Air Force has the capability to collect, analyze, produce and disseminate all-source intelligence information to support AT operations. Develop/maintain policy to ensure standardized support IAW AFI 14-119, *Intelligence Support to Force Protection (FP)*.

1.4.2.8.2. Coordinate on Air Force, DoD and Intelligence Community (IC) policies affecting intelligence support to the AT mission.

1.4.2.8.3. Maintain the ability to crosstalk with Service HHQs, MAJCOMs and AFNORTH (as the responsible C-NAF), as needed, during CONUS/OCONUS contingencies (i.e., major terrorist attacks).

1.4.2.8.4. Represent the Air Force in Director of National Intelligence (DNI), DoD and IC venues on matters of intelligence and collaborate with HQ AFOSI (SAF/IGX) and AF/A7S on AT information, policy, processes and assessments.

1.4.2.8.5. Review existing and emerging ISR system capabilities to assess their potential for AT mission support.

1.4.2.9. Operations, Plans and Requirements (AF/A3/5). AF/A3/5 shall:

1.4.2.9.1. Identify AT requirements and desired effects for mission operations.

1.4.2.9.2. Ensure operational reporting procedures for terrorist and AT-related events are established.

1.4.2.9.3. Serve as the OPR for Air Force CARM policies, processes and methodologies and approve and oversee implementation of all AF-wide and DoD Critical Infrastructure Program (CIP) requirements.

1.4.2.9.4. Ensure AT is factored into operational plans.

1.4.2.9.5. Provide guidance and expertise on those aspects of AT related to Counter-Chemical, Biological, Radiological, and Nuclear (C-CBRN) and combating WMD operations IAW AFPD 10-26.

1.4.2.9.6. As the OPR for Continuity of Operations (COOP), ensure continuity is integrated and aligned with AT to ensure the continuation of key missions and functions.

1.4.2.10. Deputy Chief of Staff Logistics, Installations, and Mission Support (AF/A4/7). AF/A4/7 is the OPR for Air Force AT policy, guidance, and instruction. AF/A4/7 shall:

1.4.2.10.1. Through the HQ USAF/A7S:

1.4.2.10.1.1. Draft and coordinate policy and guidance with the HAF FPSG and appropriate functional experts.

1.4.2.10.1.2. Develop guidance on AT and physical security enhancements.

1.4.2.10.1.3. Monitor program element (PEC) 28047 and coordinate funding for AT initiatives with Air Staff functional experts for AF/A4/7 approval.

1.4.2.10.1.4. Evaluate AT equipment and supplies.

1.4.2.10.1.5. Conduct AT VAs of USAF sites as outlined in Standard 6 in this publication.

1.4.2.10.2. Through the AF/A4L:

1.4.2.10.2.1. Provide Supply Chain Management to fulfill AT requirements.

1.4.2.10.2.2. Monitor logistics readiness of AT program support.

1.4.2.10.2.3. Manage Airmen support requirements (protective equipment, weapons, etc.).

1.4.2.10.2.4. Ensure contracting officers, in coordination with program managers and requirement officials, incorporate AT clauses required by Defense Federal Acquisition Regulation Supplement (DFARS), related supplements, and local AT measures provided as part of the requirement into AF contracts as described in AT Standard 18.

1.4.2.10.2.5. Incorporate AT considerations in the expeditionary support planning program.

1.4.2.10.3. Through the AF/A7C:

1.4.2.10.3.1. Ensure appropriate aspects of the AT Program are integrated with the Emergency Management (EM) Program as defined in AFPD 10-25, and AFI 10-2501, *Air Force Emergency Management (EM) Program, Planning and Operations*.

1.4.2.10.3.2. Serve as the OPR for crisis and consequence management aspects of homeland defense and civil support, and non-medical CBRN passive defense and consequence management programs as part of the EM program. Serve as the OPR for Explosive Ordnance Disposal (EOD) and Fire Emergency Services matters and policy.

1.4.2.10.3.3. Ensure civil engineers (CE) are included in all current and newly-developed AT policies/issues.

1.4.2.10.3.4. Provide MAJCOMs with AT guidance on new and existing

construction standards and furnish a core member to the HAF FPSG.

1.4.2.10.3.5. Provide the AF subject matter expertise on UFC AT standards.

1.4.2.11. Communications (SAF/CIO A6). SAF/CIO A6 shall:

1.4.2.11.1. Ensure net-centric communications and information (C&I), to include wireless, radio and satellite communications, identify and link Information Operations capabilities that support the AT Program and enable communications and command and control in the event of a terrorist act.

1.4.2.11.2. Provide AT policy and guidance for mail handling and management.

1.4.2.12. Deputy Chief of Staff Strategic Plans and Programs (AF/A8). AF/A8 shall:

1.4.2.12.1. Provide long-term planning and programming for AT programs and processes.

1.4.2.12.2. Develop, integrate and analyze AT initiatives for AF Future Years Defense Program (FYDP) and long range plan to support the National Military Strategy for Combating Terrorism.

1.4.2.12.3. Ensure AT programming initiatives are considered for operational impact during PPB&E processes.

1.4.2.13. Studies & Analyses, Assessments and Lessons Learned (HQ USAF/A9). AF/A9 shall provide appropriate studies and AT lessons learned from exercises and actual operations and events.

1.4.2.14. ACS Strategic Deterrence and Nuclear Integration (AF/A10). AF/A10 shall ensure that AT standards are maintained or exceeded in nuclear security standards and requirements.

1.4.2.15. Air Force Office of Special Investigations (AFOSI). AFOSI shall:

1.4.2.15.1. Conduct counterintelligence (CI) activities, to include operations, investigations, collections, services, production, and analysis of threats from terrorism.

1.4.2.15.2. Maintain liaison and serve as the AF point of contact with federal, state, local, and foreign nation law enforcement, CI and security agencies, for terrorism and other matters falling within the AFOSI mission.

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

1.4.2.15.4. Provide personal protective services for senior U.S., DoD, Air Force and allied officials.

1.4.2.15.5. Manage the USAF Non-Tactical Armored Vehicle Program.

1.4.2.15.6. Assist in the provision of AT training, to include the HRP training required by AT Standard 16.

1.4.2.15.7. Assign an AFOSI Liaison Officer to the Air National Guard Readiness Center staff.

1.4.3. MAJCOM, NAF, FOA, and DRU Staffs:

1.4.3.1. Shall manage AT Programs under their control IAW DoD Guidance, this AFI, and applicable GCC AT policies and procedures.

1.4.3.2. MAJCOM ATPMs shall oversee funds provided in PEC 28047 and coordinate funding for AT vulnerabilities identified in CVAMP and other AT initiatives.

1.4.3.3. MAJCOM Staffs shall establish an Antiterrorism Working Group (ATWG) and Antiterrorism Executive Committee (ATEC) to serve as the commander's advisory body on AT policy and program management.

1.4.3.4. The Air National Guard Readiness Center NGB/A7SO ATPM will attend the National Guard Bureau J/34 ATWG to serve as the commander's advisory body on AT policy and program management in lieu of establishing an ATWG and TWG to eliminate duplication of effort.

1.4.3.5. NAF, FOA, and DRU staffs shall participate in the host installation's ATWG to ensure their commander's AT program issues are addressed to the installation commander.

1.4.4. Installations.

1.4.4.1. AT is an installation commander responsibility and must be thoroughly integrated into every unit attached to the installation, to include tenants, sister services, and attached agencies. All installation commanders must appoint an Installation ATO, as well as wing and subordinate commanders must appoint ATRs or liaisons, as organizationally appropriate. All AT personnel must be formally designated and authorized in writing to carry out the installation AT program.

1.4.4.2. Installations shall establish an ATWG and ATEC to serve as the commander's advisory and oversight body on AT policy and program management. At the installation level the ATWG should be combined with the Integrated Defense Working Group (IDWG) and the ATEC should be combined with the Integrated Defense Council (IDC). Consider combining/including other related working groups and councils as appropriate.

1.4.4.3. Commanders at all levels shall develop working knowledge of AT policies and standards and take appropriate measures to protect DoD personnel and assets.

1.4.4.4. Force Support Squadrons (FSS) shall:

1.4.4.4.1. Serve as the OPR for incorporating and utilizing AT processes concerning food handling and distribution and will coordinate annual vulnerability assessments with Public Health for all food handling locations.

1.4.4.4.2. Assist in the review of Capability Based Manpower Standards and manpower determinant tools for appointed AT positions as described in AFI 38-201, *Management of Manpower Requirements and Authorizations.*

1.4.4.4.3. Serve as the OPR between the installation and support services tenants such as the Army and Air Force Exchange Service, Defense Commissary Agency, etc.

1.4.4.5. Contracting Squadrons (CONS) shall:

1.4.4.5.1. Coordinate contracts and contract modifications with the installation ATO to ensure AT considerations and measures are included in all applicable contracts and that all AT standards are complied with. Coordination of contract requirements should be accomplished by the requiring unit before it goes to Contracting.

1.4.4.5.2. Coordinate with the installation ATO to ensure Level I - AT Awareness Training is offered to all contractors. Coordination for training should be done by the requiring unit after contract award.

1.4.4.5.3. Provide any AT-specific contracting measures to the installation ATO for inclusion in the installation's AT Plan.

1.4.4.5.4. Coordinate necessary background investigations for contractors with Installation Information Protection Office and work with the installation ATO and the Defense Force Commander (DFC) to develop mitigation measures that limit the potential threats posed by contractors while on the installation.

1.4.4.5.5. Incorporate AT clauses required by DFARS, related supplements and local AT measures provided at part of the requirement into DoD contracts as described in DoDI 2000.16, Standard 18, AT Measures for Logistics and Other Contracting.

1.4.4.6. Communications Squadrons (CS) shall:

1.4.4.6.1. In coordination with the installation ATO, ensure vulnerabilities in information systems are entered into the CVAMP within 90 days of a signed assessment report and documented in the system security certification and accreditation package. The vulnerability must be tracked until resolved or the installation commander documents the acceptance of risk.

1.4.4.6.2. Implement AT policy and guidance for mail handling and management.

1.4.4.6.3. Coordinate CONOPS for all new installation security technologies to ensure employment and integration, requiring communication infrastructure support or network interface.

1.4.4.7. Comptroller Squadrons (CPTS) shall:

1.4.4.7.1. Assist commanders in building budget submissions to obtain AT funding (PEC 28047) for validated AT projects.

1.4.4.7.2. Work with the installation ATO to validate funding issues in CVAMP and Automated Civil Engineering System (ACES).

1.4.4.7.3. Assist the ATO in advocating for AT projects at all levels by coordinating with unit financial representatives throughout the installation.

1.4.4.8. Intelligence Unit shall:

1.4.4.8.1. Develop, implement and execute an AT support program as an integral part of the FP program. The program will identify which mission elements and functional areas, both at home and/or deployed, require intelligence support to perform their AT functions and tailor intelligence products to meet customer needs.

1.4.4.8.2. Designate intelligence personnel to participate in unit/base ATWGs, TWGs, and other force protection-associated programs/functions (e.g., IDWG and IFC), as appropriate.

1.4.4.8.3. Provide relevant terrorist threat information, products and services to subordinate units, to include GSUs, units without an organic intelligence capability, AFRC-associated units and tenant units IAW MAJCOM and C-NAF guidance.

1.4.4.8.4. Review the installation AT plan at least annually and write an intelligence annex to identify all required intelligence support and information requirements.

1.4.4.8.5. In coordination with AFOSI and/or Security Forces:

1.4.4.8.5.1. Analyze all-source intelligence information for impact on unit mission and rapidly disseminate terrorist threat information to subordinate and lateral units, HHQs and other appropriate agencies.

1.4.4.8.5.2. Establish procedures to track IC terrorist threat levels, threat warnings, alerts and advisories for threats at the home station, in deployed locations, or while in-transit to deployed locations (based on approved FP plans submitted by assigned/attached units).

1.4.4.8.5.3. Coordinate intelligence exercise activities and requirements supporting installation exercise objectives. Ensure scenarios facilitate a practical simulation of FP intelligence functions and include realistic mission area threats posed by transnational terrorists.

1.4.4.8.5.4. Support the annual development of the AFOSI Defense Threat Assessment (DTA) and local threat assessments as applicable.

1.4.4.9. Staff Judge Advocate shall:

1.4.4.9.1. Provide legal advice and guidance to the AT program.

1.4.4.9.2. Review all new support agreements such as MOUs, MOAs, or MAAs needed to support the AT program for the legal sufficiency. Thereafter, review support agreements annually.

1.4.4.10. Security Forces Squadrons (SFS) shall:

1.4.4.10.1. Ensure ID incorporates AT standards and contributes to AT planning.

1.4.4.10.2. Accomplish and maintain the Integrated Defense Risk Management Process (IDRMP) IAW AFI 31-101, *Integrated Defense (FOUO)*, with support and coordination from the installation ATO.

1.4.4.10.3. The Security Forces Commander is also referred to as the DFC throughout this instruction and is responsible for all aspects of the installation physical security and resource protection program as part of the Integrated Defense Plan (IDP) and ID effort.

1.4.4.10.4. Coordinate with the installation ATO on planning for random antiterrorism measures (RAM) to counter threat(s), mitigate vulnerabilities and reduce risk.

1.4.4.10.5. Work with the Installation ATO in presenting risk management analysis to the ATWG and ATEC to manage risk and appropriately adjust the protection posture of DoD elements and personnel.

1.4.4.10.6. In coordination with AFOSI and ATO, develop a countersurveillance/surveillance detection plan.

1.4.4.11. Civil Engineer Squadrons (CES) shall:

1.4.4.11.1. Ensure engineering infrastructure, installation and/or facility design, physical security, resource protection, fire emergency services, EOD, expeditionary engineering, and emergency management mitigation ensure projects supporting vulnerabilities identified in CVAMP are referenced and prioritized in ACES.

1.4.4.11.2. Implement terrorism incident planning for incident response, consequence management and recovery in coordination with the installation ATO and DFC.

1.4.4.11.3. Provide engineering infrastructure protection expertise to counter and mitigate terrorist threats.

1.4.4.11.4. Develop and maintain the installation barrier plan in coordination with LRS, the DFC and ATO.

1.4.4.11.5. Prepare the Design Basis Threat (DBT) IAW UFC 4-010-01, *DoD Minimum Antiterrorism Standards for Buildings* and UFC-4-020-01, *DOD Security Engineering Facilities Planning Manual* with assistance from installation planning team. The specific membership of a planning team will be based on local considerations, but in general, the following functions should be represented: Facility User, CE, ATO, Intelligence, SF, AFOSI, Operations, LRS, and CPTS.

1.4.4.11.6. Provide structural blast analysis using the Vulnerability Assessment Protection Option Program (VAPO) for all critical facilities (CARM Tiers I-III) and new and renewed leased facilities.

1.4.4.11.7. Through the Emergency Management Working Group (EMWG) develop and publish an All-Hazards Threat Assessment.

1.4.4.11.8. Serve as the Installation lead for conducting an annual CBRNE VA. Ensure vulnerabilities and observations are entered in CVAMP within 90 days of the signed assessment report. Monitor, track and manage these vulnerabilities until resolved by mitigation or installation commander's documented acceptance of risk.

1.4.4.12. Medical Group (MDG) shall:

1.4.4.12.1. Provide medical specialists (Public Health and Bioenvironmental Engineering) to the ATWG and ATEC for AT planning and assessments.

1.4.4.12.2. Serve as the installation lead for conducting annual TIC/TIM and Food/Water VAs. Ensure vulnerabilities and observations are entered in CVAMP within 90 days of the signed assessment report. Monitor, track and manage these vulnerabilities until resolved by mitigation or installation commander's documented acceptance of risk. Ensure assessment reports are formatted for entry into CVAMP.

1.4.4.12.3. Ensure local assessments per AFI 10-246 are consolidated and conducted at the same time as the local AT Vulnerability Assessment.

1.4.4.13. Installation CARM Manager shall:

1.4.4.13.1. Integrate and synchronize CARM risk management requirements, planning capabilities and guidelines, such as AF Critical Asset Management System (AF-CAMS) and Critical Asset Risk Assessment (CARA) with the installation AT program.

1.4.4.13.2. Share all threat and hazard planning information and CARM Tiers I-III critical asset-related data to support the DFC's overall IDRMP.

1.4.4.13.3. Coordinate through the CARM Working Group and installation commander to the respective MAJCOM CARM Managers in nominating and scheduling CARAs.

1.4.4.13.4. Ensure CVAMP is populated with CARA results, if required, within 90 days of the receipt of the signed assessment report. Monitor, track and manage these vulnerabilities until resolved by mitigation or installation commander's documented acceptance of risk

1.4.4.13.5. Provide other support as outlined in this AFI.

1.4.4.14. Public Affairs shall:

1.4.4.14.1. Provide communications advice and counsel to those in charge.

1.4.4.14.2. Establish procedures to handle crisis communications issues.

1.4.4.14.3. Screen information disseminated to the media to ensure operational security and force protection.

1.4.4.14.4. Provide procedures for the proper release of information during crises.

1.4.4.15. Command Post shall:

1.4.4.15.1. Conduct operational reporting IAW AFI 10-206, *Operational Reporting*.

1.4.4.15.2. Establish procedures for information dissemination from GCCs to AF components (i.e., FPCON changes, travel restrictions, advisories, etc.).

1.4.5. Installation Antiterrorism Officers (ATOs).

1.4.5.1. The installation ATO advises the installation commander on AT standards and requirements and manages the AT program at the installation level. The ATO coordinates with other staff offices to ensure the installation AT program is fully integrated with the installation IDP, emergency management plans, and medical contingency response plan (MCRP), installation and tenant continuity of operations plans and other operational/contingency plans and orders.

1.4.5.2. The installation ATO coordinates with the installation plans officer, DFC, Base Civil Engineer, communications officer, medical, and others to ensure that AT program requirements and considerations are factored into planning for programs under their control and authority.

1.4.6. Unit AT Representatives (ATR). ATRs are charged with advising their unit commander on AT issues and managing the AT Program for their unit or DoD element and personnel. Requirements for a unit/DoD element to have an ATR and their responsibilities are outlined in AT Standard 9.

Chapter 2

ANTITERRORISM STANDARDS

2.1. Standard 1: AT Program Elements. The minimum required elements of an AT program shall be: risk management (Standard 3); planning (including development of the AT Plan) (Standard 7); training and exercises (Standard 23); resource application (Standard 30); and comprehensive program review (Standard 31). The development and maintenance of the AT Program elements should be ongoing and continuously refined to ensure the relevance and viability of all measures employed to reduce vulnerabilities to terrorism.

2.2. Standard 2: Intelligence Support to the AT Program.

2.2.1. At the national level, the Defense Intelligence Agency (DIA) sets the DoD Terrorism Threat Level (TTL). This threat level identifies the potential threat to DoD interests in a particular country, including the United States. The DoD TTL applies whether or not U.S. personnel are present in the country. GCCs may also set terrorism threat levels for specific personnel, family members, units, installations or geographic regions in countries within their AOR. See Attachment 3 for more information on TTLs.

2.2.2. Commanders of MAJCOMs, AF Components to the GCC, C-NAFs, NAFs, wings, installations or separate facilities, and deployed commanders assigned AT responsibility shall:

2.2.2.1. Task the appropriate officials under their command or control to gather, analyze and circulate appropriate terrorism threat information while ensuring all applicable Intelligence Oversight (IO) rules are followed. When local information indicates gaps, commanders shall forward timely requests for information via appropriate intelligence collection and production channels.

2.2.2.2. Identify an Intelligence official as the lead force protection intelligence (FPI) representative.

2.2.2.3. Identify an AFOSI official as the focal point for local or host nation law enforcement intelligence, CI and criminal information.

2.2.2.4. Ensure Intel and AFOSI, in coordination with the TWG, develop AT Priority Intelligence Requirements (PIRs) for integration into the Commander's Critical Information Requirements (CCIRs) to focus collection and analysis efforts in support of installations and units. (NOTE: IO rules apply to CONUS-related PIRs.) Coordinate AT-related requirements, products and services with appropriate AFOSI regions, MAJCOM security forces and Operations personnel, and appropriate critical asset risk management assessors.

2.2.2.5. Establish guidance for, program for, allocate resources for, and provide management for all command AT-related intelligence requirements. MAJCOMs should tailor their responsibilities based upon AT customer requirements, location and mission/area of operation.

2.2.2.6. Develop and implement an Intelligence Support to AT program in coordination with the supported Combatant Command (COCOM) air components, C-NAF, AFOSI

Region, and MAJCOM staff elements (e.g., A2, A3/A5 and A4/A7). Ensure units in-transit are provided with tailored terrorist threat information.

2.2.2.7. Establish procedures to rapidly receive, evaluate, analyze and disseminate all relevant intelligence threat data with AFOSI, SF and other Staff Force Protection elements. Ensure procedures are established to track IC terrorism threat levels, terrorism warnings, alerts and advisories.

2.2.2.7.1. Incorporate proactive techniques to detect and deter terrorists, particularly in support of assets or activities conducted in areas designated with SIGNIFICANT or HIGH TTLs. These activities shall include, but are not limited to: In-transit forces, HRP, CARM Tier I and II critical assets, special events and high-value military cargo shipments.

2.2.2.7.2. Ensure all levels of subordinate elements forward up and down the chain of command all information pertaining to suspected terrorist threats or acts of terrorism involving DoD elements and personnel or assets for which they have responsibility, including the provisions to provide such information to appropriate interagency officials.

2.2.2.7.3. Assess subordinate intelligence organizations' ability to receive, evaluate, analyze, and disseminate all relevant data on terrorist/extremist activities, trends, and indicators of imminent attack.

2.2.2.8. Direct membership within the appropriate ATWG, TWG and other force protection-related working groups as applicable.

2.2.2.9. Ensure Intelligence for the AT Program is provided by organic Intelligence elements IAW AFI 14-119, AFPAM 14-118, *Predictive Battlespace Awareness: Air and Space Intelligence Preparation of the Operational Environment*, and all relevant guidance and doctrine.

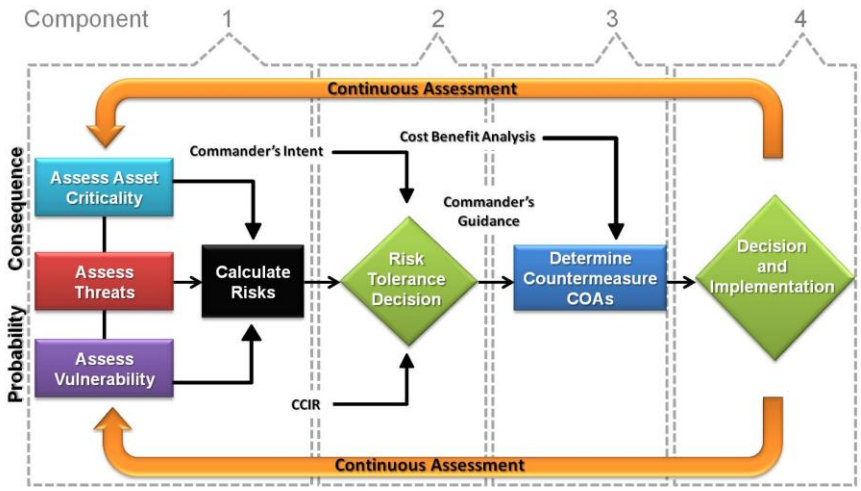
2.2.3. Air Force intelligence, CI and law enforcement elements will coordinate the dissemination of information on U.S. persons as appropriate in support of the AT Program and within the provisions of AFPD 71-1; AFI 71-101, Volume 1, *Criminal Investigations Program*; DoD 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*; and AFI 14-104, *Oversight of Intelligence Activities*.

2.3. Standard 3: AT Risk Management. AT risk management shall be applied in all aspects of AT program implementation and planning, including operational plans and decisions, development of risk mitigation measures and the prioritization and allocation of resources. The essential components of risk management include: determining the criticality of assets (criticality assessment); assessing the terrorist threat (threat assessment); identifying the vulnerabilities of facilities, programs and systems to an attack, including the use of CBRNE (including TIC/TIM) or similar capabilities (vulnerability assessment); assessing risk based on a holistic understanding of the criticality, threat and vulnerability of the asset (risk assessment); and implementing the actions needed to correct or mitigate the risk (countermeasures) and reevaluating risk after countermeasures are employed and/or documenting the commander's acceptance of the risk.

2.3.1. AT programs shall employ the IDRMP process IAW AFI 31-101, to assess the risk to the installation or facility, because of the presence of terrorist threats, annually or as changes occur.

2.3.2. Risk management is a continuous process. The risk management process and procedures shall be reviewed by the ATWG and approved by the ATEC annually or as changes occur. See Figure 2.1 for a graphic depiction.

Figure 2.1. AT Risk Management Process



2.4. Standard 4: Terrorism Threat Assessment.

2.4.1. The threat assessment process shall be established consistent with the IDRMP outlined in AFI 31-101, to identify the full range of known or estimated threat capabilities (including the use or threat of CBRNE). These assessments shall be updated on an annual basis or more frequently as the threat environment dictates, or upon changes to the DIA or GCC TTL. Assessments shall be tailored to local conditions. For each group that may pose a threat, at a minimum, the assessment shall provide the following information: the group's intent, tactics, techniques and procedures (TTP), capability, probable course of action (COA), history, and any specific targeting information that may be available. AFOSI is the AF agency responsible for preparing the DTA as prescribed in DoDI 5240.18, *Counterintelligence (CI) Analysis and Production*; DoD O-2000.12-H; and AFI 71-101, Volume 4, *Counterintelligence*.

2.4.1.1. A DBT shall be established for each installation to identify and evaluate the various weapons and tactics most likely to be used by terrorist groups. The DBT will be used to help establish the base's defensive posture and is critical for engineering projects and renovations. In the absence of a credible threat, the baseline UFC standards can be used as the installation's DBT.

2.4.2. Specific threat assessments are also prepared to support operational planning and risk decisions for unique mission requirements or special events including, but not limited to, in-transit forces, training and exercises, and operational deployments. AFOSI is responsible for preparing specific threat assessments.

2.4.3. Effective processes should be implemented to integrate and fuse all sources of available threat information from local, State, Federal and host nation law enforcement agencies; the appropriate local, State, Federal and host nation intelligence community activities; other local community officials and individuals; the applicable U.S. country team; port authority officials and husbanding contractors, as appropriate, to provide for a continuous analysis of threat information to support the threat warning process IAW Standard 2.

2.4.4. Threat assessments are integrated into the AT risk management process as a major source of analysis and justification for recommendations and implementation of Random Antiterrorism Measures (RAMs); AT enhancements, including physical security, emergency management or FHP changes; program and budget requests; and when conducting AT VAs.

2.4.5. Other targeted Threat Assessments will be reviewed by the TWG and incorporated into AT planning.

2.5. Standard 5: Criticality Assessment.

2.5.1. Criticality assessment processes shall be conducted IAW the IDRMP outlined in AFI 31-101, to identify, classify and prioritize missions, including mission-essential personnel, assets and information.

2.5.1.1. Criticality assessments shall also be conducted for non-mission essential assets such as primary gathering buildings (routinely occupied by 50 or more DoD personnel), special events (involving 300 or more DoD members), energy infrastructure and any other facility, equipment, service or resource deemed important by the commander warranting protective measures to ensure continued efficient operation, protection from disruption, degradation or destruction, and timely restoration. Additional guidance for criticality assessments can be found in DoD Antiterrorism Handbook.

2.5.1.2. Criticality assessments shall be updated at least annually to determine the degree of asset criticality. Criticality assessments shall provide the basis for identifying those assets that require specific protective measures and priorities for resource allocation when developing and updating AT-related plans [e.g., AT Plan, Comprehensive Emergency Management Plan (CEMP) 10-2, Contingency Response Plan (CRP), MCRP, IDP, etc.].

2.5.2. Criticality assessments should be coordinated with affected Defense Critical Infrastructure Program (DCIP) and Air Force CARM, and conducted IAW the principles in DoDD 3020.40, *DoD Policy and Responsibilities for Critical Infrastructure*, and AFPD 10-24, *Air Force Critical Infrastructure Program (CIP)*, and identify defense critical infrastructure and critical assets. Criticality assessments for DCIP and AF CARM assets will be conducted IAW DoDI 3020.45, *Defense Critical Infrastructure Program (DCIP) Management*; DoDM 3020.45, Volume 1, *Defense Critical Infrastructure Program (DCIP): DoD Mission-Based Critical Asset Identification Process (CAIP)*; DoDM 3020.45, Volume 5, *Defense Critical Infrastructure Program (DCIP): Execution Timeline*, and AF implementing publications on a biennial basis or immediately as changes occur.

2.6. Standard 6: Terrorism Vulnerability Assessment. VA processes will be conducted per DoDI 2000.16 or DoD O-2000.12H. VA results will be used IAW AFI 31-101 to provide a vulnerability-based analysis of personnel (mission essential, mass gatherings, etc.), mission essential assets (energy, infrastructure, etc.), and information susceptible to all threats and

hazards. All assessment OPRs will coordinate and conduct other wing assessments during the Installation Vulnerability Assessment, (e.g., Food, Water, Toxic Industrial Chemicals/Toxic Industrial Material [TIC/TIM], CBRNE and DCIP assessments) to reduce the impact on operational units.

2.6.1. DoD and COCOM benchmarks will be used to guide all AF VAs. The Installation's IDRMP shall be used to focus VAs when evaluating the installation against DoD/COCOM benchmarks to ensure appropriate criticality and threat factors are considered, unless directed otherwise by the GCC.

2.6.2. A VA will be conducted at least annually or as threat or mission requirements dictate. Installation ATOs shall report completion of their Local VA to their higher headquarters. Completed VA reports shall be entered into CVAMP and reviewed by the MAJCOM. VAs shall be conducted at a minimum for, but not limited to:

2.6.2.1. Any AF installation or AF owned or leased facility populated daily by 300 or more DoD personnel.

2.6.2.2. Any AF installation or facility bearing C2 responsibility for emergency response or physical security plans and programs; determined to host defense critical infrastructure or critical assets identified through the DCIP or AF CARM; or using, possessing, transferring, or receiving biological select agents and toxins (refer to DoDI 5210.89_AFI 10-3901, *Minimum Security Standards for Safeguarding Biological Select Agents and Toxins*).

2.6.2.3. Any AF installation, facility, or activity involving interaction with local non-military or host nation agencies.

2.6.2.4. AF-hosted air ports of embarkation (POE) and debarkation (POD); movement routes (air, ground and rail); and assembly, staging, reception and final bed down locations in support of any battalion, squadron, ship, or equivalent operational deployment; and similar sized in-transit movement or training exercise. AF movement or shipment of military cargo shall be coordinated with the designated senior DoD Component with AT responsibility.

2.6.2.5. Any AF personnel designated as HRP (Standard 16). These assessments are referred to as Personal Security Vulnerability Assessments (PSVAs). PSVAs will conform to the formats of servicing Protection Providing Organizations (PPO) as identified in DoDI O-2000.22, *Designation and Physical Protection of DoD High Risk Personnel (HRP)*. AFOSI is a designated PPO.

2.6.2.6. Any AF event or activity determined to be a special event involving a gathering of 300 or more DoD personnel. Consider creating a Special Events Assessment Plan or Template tailored for such activities.

2.6.2.7. AF-owned or leased off-installation housing, schools, daycare centers, commissaries, transportation systems and routes used by DoD personnel and their dependent family members when the TTL is SIGNIFICANT or higher, consistent with Standard 3. At locations where there are multiple DoD components or locations that are not AF-owned or leased, VA requirements shall be coordinated with the designated senior DoD Component with AT responsibility.

2.6.3. A VA of installations or facilities with 300 personnel or more on a daily basis shall be conducted by a HHQ team triennially (refer to AFI 10-246 for Food and Water VA).

2.6.4. Information derived from AT VAs shall be classified pursuant to the requirements outlined in the Defense Threat Reduction Agency (DTRA) Security Classification Guide for Vulnerability Assessments. Information related to DCIP assets shall be classified pursuant to the requirements outlined in the DCIP Security Classification Guide.

2.6.5. AT vulnerability assessments conducted by the local installation, the AF VA Team (AFVAT), or any other HHQ level, shall include a review of any vulnerability or concern identified in a previous VA (from any source/level) which remains open (i.e., not “accepted” or mitigated).

2.6.6. Mitigation Plan. Within 90 days of a signed assessment report, a mitigation plan addressing any identified vulnerabilities will be developed and released to the first general officer, flag officer or civilian equivalent director in the chain of command. The mitigation plan shall be staffed or submitted through CVAMP and include: vulnerability identification and prioritization; likely threats/hazards associated with the vulnerability; impact if vulnerability is exploited; action plan to eliminate or reduce risk to an acceptable level and the anticipated residual risk to be accepted by the commander; estimated completion date of the action plan; and resources required.

2.6.7. CVAMP shall be populated with all assessment results within 120 days of the signed assessment report (Neutral and Positive observations are not required to be loaded into CVAMP). Within 240 days of a signed assessment report, all observations must be updated with a plan of mitigation or closed with Commander's risk acceptance. When populating CVAMP, at a minimum attach a copy of the applicable VA outbrief and final report to the record created in CVAMP.

2.6.7.1. HHQ shall take action (release or return) on appropriate observations within 30 days of installation submittal.

2.6.7.2. Installation ATOs, in conjunction with vulnerability/observation OPR or functional SME, will review and update CVAMP quarterly. The ATWG and ATEC will review open CVAMP vulnerabilities and concerns semi-annually.

2.6.7.3. Installation Commanders may authorize Installation ATO's "Commanders Privileges" within CVAMP to aid in database maintenance. Such authorization will be in writing, and may be included on the ATO appointment letter. However, this does not relieve the commander from having situational awareness of the data within CVAMP.

2.6.8. Triennial HHQ VA scheduling for AF installations or assets will be coordinated by the AF VAT annually. HHQ VAs will only be scheduled for the next fiscal year due to limitations put in place by DTRA and COCOM scheduling processes which take precedence over AF scheduling guidance. It is incumbent on MAJCOM ATPMs to nominate installations or assets that meet the criteria in para 2.6.2. through their MAJCOM IG Gatekeepers to the AF VAT. Nominations for the next fiscal year must be submitted to the AF VAT by 15 February to ensure adequate time for de-confliction and submission to DTRA and COCOM annual calls for nominations. Once DTRA and COCOM schedules for the next fiscal year are set, the AF VAT will work with the appropriate MAJCOM IG Gatekeepers and ATPMs to complete any HHQ VA not covered by DTRA or COCOM teams. When the

AF VAT is available, AF VA will be conducted in conjunction with MAJCOM Phase 0 Inspections. Since the AF VAT is a low density/high demand team, AF VA will not be scheduled to occur more than 6 months ahead of or behind an installation's triennial due date for the sole purpose of aligning with MAJCOM inspections.

2.6.8.1. The AF VAT scheduling process will incorporate AF CARM Critical Asset Risk Assessment (CARA) requirements. Where possible, AF CARAs and AF VAs will be aligned to assess an installation at the same time to produce a more comprehensive product and minimize impact on the installation.

2.6.8.2. Once a HHQ VA schedule has been published, MAJCOMs and installations should make every effort to abide by the schedule. Cancellations and schedule changes are sometimes costly and difficult to facilitate. Cancellation request procedures for JSIVA will be identified in the DTRA call for nominations message. Cancellations for COCOM/MAJCOM HHQ VA teams will be IAW COCOM/MAJCOM guidance. Cancellations for AF VAs require written justification from the installation Wing Commander through the owning MAJCOM IG to the Commander, HQ AFSFC. The request should include the circumstances which require the assessment cancellation or schedule change and proposed alternate dates. If the AF VAT is unable to accommodate rescheduling the assessment, the MAJCOM is responsible for either completing the HHQ VA with an internal team or working with DTRA or their assigned COCOM to complete the assessment.

2.6.8.3. HHQ VAs conducted by NAF or MAJCOM VA teams will be reported to the AF VAT for tracking and scheduling purposes. Additionally, VA Reports from these assessments will be provided to, and tracked by, the AFVAT.

2.6.8.4. HHQ VAs will be considered complete when signed by the appropriate HHQ authority.

2.6.9. MAJCOMs and AF Components to the GCC will support the GCCs in scheduling assessments and prescribing policies for no-notice or short-notice movements to locations where a VA has not been accomplished or is not current. MAJCOM ATPMs will receive copies of reports on all VAs completed based on Standard 6.

2.6.10. Headquarters Air Force Security Forces Center (HQ AFSFC)/SFOZ (VA) shall provide the HAF FPWG a semi-annual vulnerability and concerns trend report based upon AF VAT reports. MAJCOM ATPMs shall provide units within their command a semi-annual vulnerability and concerns trend update based upon MAJCOM and HHQ Vulnerability Assessment reports. In addition, MAJCOM ATPMs shall review Installation CVAMP entries semi-annually.

2.6.11. Local vulnerability assessment team composition can be tailored to the installation needs. The assessment team should consist of a team chief, physical security specialist, structural/infrastructure engineer, terrorist operations specialist, emergency management specialist, medical operations specialist, communications specialist and EOD specialist, when appropriate. Other functional experts may augment the team as needed, depending on the type of assessment required (comprehensive or targeted), the nature of the installation's mission, and the terrorist threat level.

2.7. Standard 7: AT Plan.

2.7.1. Installation Commanders will develop and maintain a comprehensive AT plan for all elements and personnel for which the AF has AT responsibility. Installation AT plans must be cross-referenced, compatible, and synchronized with other base plans (IDP, CEMP, MCRP, etc.). AT plans will not be considered complete unless signed by the commander and exercised. At a minimum, AT plans shall be developed for the installation (integrating separate/leased facilities), for AF operational deployments, training exercise deployments or events, and special events.

2.7.1.1. Installation AT plans will specify requirements for unit AT plans and programs. Air National Guard (ANG) and Air Force Reserve (AFR) tenant units will be integrated into host installation AT plans, and are not required to write their own. However, they will develop an AT plan or instruction for their unit detailing unit procedures based on the host installation's AT plan. ANG and AFR tenant units will appoint an ATR for each unit and will participate fully in the host installation's AT program.

2.7.1.2. Installation Commanders will review and sign AT plans within 60 days of taking command.

2.7.2. AT principles are incorporated into all operational plans and risk decisions using the standards prescribed by this instruction as a baseline to develop and implement AT policies in support of the AF's unique roles and mission requirements. Table 2.1. incorporates Presidential Policy Directive (PPD) 8, *National Preparedness*. The OPR will recommend the appropriate planning parameters regarding the scale for AF operations and civil support operations based on the threat. Where A7C (CE) is designated the OPR, refer to AFI 10-2501.

Table 2.1. AT Threat Planning Scenarios

Scenario	Title	OPR
1	Nuclear Detonation – 10-Kiloton Improvised Nuclear Device	A7C (CE)
2	Biological Attack – Aerosol Anthrax	A7C (CE)
4	Biological Attack – Plague	A7C (CE)
5	Chemical Attack – Blister Agent	A7C (CE)
6	Chemical Attack – Toxic Industrial Chemicals	A7C (CE)
7	Chemical Attack – Nerve Agent	A7C (CE)
8	Chemical Attack – Chlorine Tank Explosion	A7C (CE)
11	Radiological Attack – Radiological Dispersal Devices	A7C (CE)
12	Explosive Attack – Bombing Using Improvised Explosive Devices	A7C (CE)
13	Biological Attack – Food Contamination	(Medical)
15	Cyber Attack	CIO/A6 or

		AFNetOps
16 (AF)	Armed Attack – Small Arms: Indiv to 10 pers (includes active shooter)	A7S (SF)
17 (AF)	Attacks on Aircraft in the Take-off and Landing Footprint	A7S (SF)
18 (AF)	Stand-off Indirect Fire	A7S (SF)
19 (AF)	Sniper Attack	A7S (SF)
20 (AF)	Hostage Crisis	A7S (SF)
21 (AF)	Contamination of Drinking Water System	SG3 (Medical)
22 (AF)	Extended Loss of Energy Supply	A7C (CE)
Note: Scenarios are numbered to correspond to the national scenarios, except for AF added scenarios.		

2.7.3. Tailor AT plans to the level of command or activity for which the AT principles were developed. AT plans should reference (not copy) information in other base plans. At a minimum AT plans shall address:

2.7.3.1. The minimum essential AT program elements (AT Standard 1) and standards prescribed by this instruction to include:

2.7.3.2. Risk correction or mitigation measures to establish a local baseline defensive posture. The local baseline defensive posture shall facilitate systematic movement to and from elevated security postures, including the application of RAMs.

2.7.3.3. AT physical security measures (Standard 13). These measures, to include the barrier plan, will be contained within the IDP and referenced in the AT plan.

2.7.3.4. AT risk mitigation measures for AF off-installation facilities, housing and activities (Standard 15).

2.7.3.5. AT risk mitigation measures for HRP (Standard 16).

2.7.3.6. AT construction and building considerations (Standard 17).

2.7.3.7. AT risk mitigation measures for logistics and other contracting (Standard 18).

2.7.3.8. AT risk mitigation measures for critical asset security (Standard 19).

2.7.3.9. AT risk mitigation measures for in-transit movements.

2.7.3.10. AT incident response measures (Standard 20).

2.7.3.11. Terrorism consequence management measures, including CBRNE mitigation planning (Standard 21 and CEMP 10-2).

2.7.3.12. FPCON implementation measures, including site-specific AT measures (Standard 22).

2.7.4. AT planning information (e.g., airfield, port, and movement route information and criticality, threat, and VA data) for deploying DoD units may be provided by GCCs. GCCs may also direct the execution of advance site surveys to facilitate the AT planning process in

areas where the assessed TTL is SIGNIFICANT or HIGH or where a specific terrorism warning is in effect.

2.7.4.1. At the discretion of the GCC, such security efforts may be waived for deployments or visits to controlled locations such as existing military installations.

2.7.4.2. Augmentation of assessment personnel may be necessary to enable subordinate AF Component commanders to discharge their responsibility to provide security, surveys, assessments, CI and countersurveillance support, and to act as the liaison with the country team, host nation security force, contractors and port authority.

2.7.5. In countries where available, AFOSI special agents are assigned to FP Detachments (FPD) and provide FP and CI services to in-transit DoD personnel. FPDs are mandated to provide surveys, assessments, CI and countersurveillance support, and act as the liaison with the country team, host nation security forces, contractors and port authority.

2.7.6. Coordinate AFOSI support for large exercises, contingencies and special events in foreign countries.

2.7.7. Ensure plans include procedures to expedite responding off-base (civilian and military) first and emergency responders onto the installation during emergencies, under all FPCONs.

2.8. Standard 8: AT Program Coordination.

2.8.1. GCCs coordinate AT and security matters with the appropriate CoM and host nation authorities for countries within their AOR and with the heads of the other DoD Components whose personnel are stationed in or transit the respective GCC AOR.

2.8.2. AF Component commanders of personnel who will be stationed in or transit the AOR of a GCC shall:

2.8.2.1. Initiate coordination of AT matters with the appropriate GCC pursuant to the requirements established by DoDI 2000.12.

2.8.2.1.1. The senior deployed commander with AT responsibility will designate an ATO in writing to coordinate with the AF Component to the GCC and provide this information through the Unit Deployment Centers with Unit Type Codes (UTCs) assigned for the deployment.

2.8.2.1.2. AF elements of in-transit forces with less than 300 personnel and not deploying as a larger troop movement will comply with the GCC operation order (OPORD) and file an in-transit AT plan with their ATO and commander for approval. This requirement will typically apply to troop movements of 50 or more personnel; however, commanders may lower this threshold at their discretion based on threat or other considerations. Coordinate with MAJCOMs or GCCs to determine additional in-transit AT plan filing requirements. The plan will cover travel from permanent station to the initial assembly or embarkation point, where it becomes the responsibility of the senior officer of a larger movement, such as a troop commander. If the movement does not join a larger force where AT responsibility is transferred, the AT plan must include transit to the deployed location where a commander is designated as having AT responsibility by orders.

2.8.2.1.3. For countries where the AF will be performing temporary duty, commanders will immediately contact the AFOSI unit or ATO responsible for that AOR. AFOSI will provide a specific, tailored threat briefing prior to departure.

2.8.2.2. Coordinate AT matters with local, State, Federal, Tribal, and/or host nation authorities pursuant to existing law, AF and DoD policy to support AT planning and implementation. Where support agreements such as MOUs, MOAs or MAA are needed to support the AT program, ensure they are reviewed annually by the ATWG for currency and executability, and exercised annually (all parties to the agreement should participate in at least one exercise annually).

2.8.3. All tenant units, DoD elements, and privatized support to AF property and activities shall coordinate AT program and plan requirements with the host installation commander or civilian equivalent director. Tenant units, DoD elements, support activities, and separate facilities shall participate fully in the host installation's AT program, to include participation in AT exercises. At locations where there are multiple DoD components, such as DoD-leased facilities or other facilities where DoD occupies space, the designated senior DoD Component, unless otherwise stipulated by the applicable GCC, shall be responsible for integrating and coordinating individual DoD component security plans into a comprehensive installation, separate facility or area-wide AT program.

2.9. Standard 9: AT Officer (ATO).

2.9.1. Commanders will designate, in writing, a Level II-qualified commissioned officer, non-commissioned officer, or civilian staff officer as the ATO (see Standard 26 for criteria). The ATO is the commander's military or civilian advisor charged with managing the AT Program (contractors may not be appointed as primary or alternate ATO for government facilities). The ATO advisory role does not replace a functional manager's or commander's responsibility to execute programs in support of the operational commander's mission. ATOs shall be assigned to:

2.9.1.1. Installation and separate facility (those not supported by a host installation AT Program) or higher levels.

2.9.1.2. Units having 300 or more personnel assigned or under the operational control of a designated commander will have a Level II-certified ATO.

2.9.1.3. Units with an authorized strength of 299 or fewer and separate flights/elements will have a unit ATR appointed in writing by the unit commander or element chief. The Installation Commander will determine how their staff agencies and personnel will be consolidated. Unit ATRs will hold a minimum grade of SSgt (E-5) or civilian equivalent.

2.9.2. All ATOs/ATRs (irrespective to level assigned) shall:

2.9.2.1. Assist the commander in implementing Joint, DoD, GCC and Air Force AT-related doctrine, policy and TTPs. Make recommendations to the commander if supplemental policy and guidance is necessary to execute the commander's AT Program.

2.9.2.2. Recommend guidance, priorities and resourcing strategies for the correction or mitigation of AT vulnerabilities to the ATEC.

2.9.2.3. Review and recommend CCIF submissions to correct or mitigate emergency or emergent AT vulnerabilities through the AF Component to the GCC IAW Chairman of

the Joint Chiefs of Staff Instruction (CJCSI) 5261.01F, *Combating Terrorism Readiness Initiative Fund*, or CJCSI 7401.1, *Combatant Commander Initiative Fund*, and GCC instructions.

2.9.2.4. Provide AT considerations, to include real-world and exercise lessons learned, to assist the installation/facility exercise evaluation team (EET) in developing realistic and relevant scenarios to exercise and validate the AT program.

2.9.2.5. Collaborate with the TWG to determine if action through warnings, policy & guidance, or organize, train and equip functions are necessary based on worldwide terrorism incidents or threats. The ANG collaborates with the NGB/J34 TWG to determine if action through warnings, policy & guidance, or organize, train and equip functions are necessary based on worldwide terrorism incidents or threats.

2.9.2.6. Work closely with AFOSI and Security Forces to support and advocate the Air Force Eagle Eyes program.

2.9.2.7. Participate in installation working groups such as the IDWG, ATWG, TWG, EMWG, CARMWG, Facilities Board, and Medical working groups as necessary.

2.9.3. The following are the requirements and responsibilities for installation and wing-level (and higher) ATOs:

2.9.3.1. The minimum grade of these ATOs shall be O-3, E-7, GS-12 or equivalent. At units or deployed locations where the rank requirements cannot be met, the priority for selecting an ATO should be based on AT expertise and certification. In order to effectively coordinate on threat data with AFOSI and A2 Force Protection Intelligence (FPI) representatives, the Installation ATO requires appropriate clearance and access to Top Secret (TS), Sensitive Compartmented Information (SCI), and Human Intelligence (HUMINT) Control System (HCS) and Gamma (G) data. Individuals requiring these clearances will work through their unit and MAJCOM A1 to change their Unit Manning Document (UMD) position(s) to reflect the needed clearances.

2.9.3.2. Installation ATOs will be assigned to the commander's immediate staff for access to the commander or a senior officer on the commander's immediate staff.

2.9.3.3. Ensure CVAMP is populated with all observations from assessments and program review reports IAW this instruction. Additional functional databases may be used for follow-on project information and tracking, but a reference note must be documented in the vulnerability observation within CVAMP. Coordinate with functional commanders to ensure AT-related observations (vulnerabilities and concerns) are entered in, and decisions or actions are tracked in, CVAMP.

2.9.3.4. Ensure CVAMP is used to identify and track AT resourcing actions and appropriate vulnerabilities are submitted to the owning MAJCOM or HHQ for AT funding assistance. Where emergency or newly-emergent requirements occur, recommend and document requests/concerns for CCIF funding IAW para 2.9.2.3. of this publication.

2.9.3.5. DCIP and AF CARM critical asset data and CARA after-action reports will be populated and tracked by the CARM Manager in AF-CAMS.

2.9.3.6. Monitor and manage funds provided in PEC 28047 and coordinate funding for AT vulnerabilities identified in CVAMP and other AT initiatives.

2.9.3.7. Assist the DFC's staff in facilitating AT issues before the IDWG or ATWG and IDC or ATEC.

2.9.3.8. Coordinate with intel and AFOSI representatives to ensure the commander's CCIRs and PIRs are developed.

2.9.3.9. Assist the CES in the development of DBTs

2.9.3.10. Coordinate for local and HHQ VAs.

2.9.3.11. Coordinate multifunctional teams of Subject Matter Experts (SMEs) when conducting required AT assessments (Vulnerability, Criticality, and Threat Assessments). Provide results of each assessment to the designated Security Forces POC for inclusion in the Integrated Defense Risk Management Process (IDRMP)

2.9.3.12. In conjunction with unit ATRs and functional representatives, facilitate interaction for developing plans and programs that support seamless capability application and de-confliction of resources for terrorist incident management.

2.9.3.13. Direct the installation RAM program in close coordination with the installation DFC.

2.9.3.14. Provide ATRs with electronic and/or hardcopy materials for use in unit continuity binders. Consider utilizing technology (i.e., SharePoint, Community of Practice, Shared Drives, etc) to establish electronic master continuity books to facilitate updates and standardization of unit binders.

2.9.4. The following are the responsibilities for unit-level ATRs:

2.9.4.1. Ensure FPCONs are implemented and report status to the installation or separate facility ATO as prescribed in the installation or separate facility AT plan.

2.9.4.2. In coordination with the Unit Training Monitor, track unit members' completion of initial and annual-refresher Level I - AT Awareness Training and update the unit commander on compliance.

2.9.4.3. Assist the unit deployment officer in attaining pre-deployment country threat briefs for deploying personnel if not provided through the Unit Deployment Center.

2.9.4.4. Assist in scheduling and tracking RAM implementation within their unit and provide this information to the installation or separate facility ATO as prescribed in local guidance.

2.9.4.5. Assist the installation ATO with AT Program implementation, where applicable.

2.9.4.6. Ensure unit personnel (military and civilian) receive appropriate threat awareness information prior to departing the Continental United States (CONUS), or if traveling OCONUS between countries. Encourage the same for dependent family members.

2.10. Standard 10: AT Working Group (ATWG).

2.10.1. Multi-functional ATWGs shall be established at AF installations and self supported separate facilities, AF-managed facilities, and higher headquarters that meet at least semi-annually or more often if needed to address AT program issues. ATWGs oversee the implementation of the AT program, develop and refine AT plans and address emergent or emergency AT program issues, and review open vulnerabilities and concerns. The ATWG recommends COAs to the ATEC; develops AT-related policy, TTPs and guidance; clarifies AT roles and responsibilities; conducts long-range planning and recommends resourcing requirements; and addresses emergent or emergency requirements through the CCIF or CbT RIF.

2.10.1.1. At the installation level, the ATWG should be combined with the Integrated Defense Working Group (IDWG), refer to AFI 31-101. Ensure meeting minutes clearly identify AT-related agenda items so that a record is maintained of AT-related meetings, decisions, discussions and activities.

2.10.1.2. Maintain a minimum of the last 12 months of meeting minutes on file. Coordinate with other working groups as appropriate to eliminate redundant records/efforts. Units will ensure they allow for local Table and Rule within their respective file plans and maintain this reference data for unit continuity and action as required.

2.10.2. The chairperson for the ATWG will be designated by the Installation Commander. The ATWG is usually composed of the ATO, DFC, CARM Manager, Intelligence, AFOSI, and Emergency Management. Consider including other functional level expertise and appropriate representation from external Law Enforcement agencies and the Intelligence Community as needed. The chair and mandatory members of the ATWG will be designated in writing by the installation commander. Security clearance requirements for members also will be established by the installation commander.

2.10.3. At the HAF level, the ATWG is combined with the Force Protection Working Group (FPWG). AF/A7SO chairs the HAF FPWG. The HAF FPWG is an action officer-level group, meeting semi-annually, or more frequently as needed, to work FP issues as directed by the HAF FP Steering Group, and to coordinate and integrate Force Protection efforts among the members, to include AT efforts. Similar procedures should be implemented at the MAJCOM level.

2.11. Standard 11: Threat Working Group (TWG).

2.11.1. A multi-functional TWG shall be established at AF installations, self supported separate facilities, and higher headquarters which meets as needed to analyze and counter an emergent threat. The TWG is required to meet at least quarterly or more frequently, depending upon the threat activity. The TWG should be activated at least semiannually in response to Wing level Antiterrorism exercises. TWGs develop and refine terrorism threat assessments and coordinate and disseminate threat warnings, reports, and summaries.

2.11.2. The TWG will be chaired by the installation commander (or a designated representative) and is composed of the DFC, ATO, Intelligence, AFOSI, Security Forces (S2) (identified in AFI 38-101), Public Affairs, and Legal (additional membership can be added

based on the threat). Security clearance requirements for members will be established by the commander.

2.11.3. The Information Fusion Cell (IFC) as identified in AFI 31-101 may be leveraged to fill threat information gaps in order to facilitate the COA development process.

2.12. Standard 12: AT Executive Committee (ATEC).

2.12.1. An AT executive-level committee will be established at AF installations, self supported separate facilities, and higher headquarters that meets at least semi annually or as directed by the commander (i.e., emerging threats, IDRMP, etc.). The goal of the ATEC is to develop and refine AT program guidance, policy and standards; act upon recommendations of the ATWG; and determine resource allocation priorities to mitigate or eliminate terrorism-related vulnerabilities.

2.12.2. The ATEC will be chaired by the installation commander (or a designated representative) and is composed of the group commanders (or designated representatives), and is supported by the ATO, DFC, Intelligence, AFOSI, Security Forces (S2), Communications, Information Protection, Emergency Management, Critical Infrastructure, EOD, Logistics Readiness, Medical Readiness, Public Affairs, Legal, Air Field Operations, Financial Management, major tenants, and supported Components on a Joint Base consistent with parent Service directives and local MOUs. The chair and mandatory members of the ATEC will be designated in writing. Security clearance requirements for members will be established by the commander.

2.12.3. On AF installations and self supported separate facilities, the ATEC should be combined with the IDC. Ensure meeting minutes accurately identify which decisions and areas of discussion are related to the installation AT program. Maintain at least the past 12 months of meeting minutes on file. Coordinate with other working groups to eliminate redundant records/efforts. Units will ensure they allow for local Table and Rule within their respective file plans to maintain this reference data for unit continuity and action as required. The ATEC will conduct a semi-annual review of all AT deviations, local FPCON measures, Installation Risk Assessments, open CVAMP observations, Wing AT plan and Wing RAM execution.

2.12.4. At the Headquarters Air Force level, the ATEC shall be constituted within the HAF FPSG. AF/A7S chairs the HAF FP Steering Group. The HAF FPSG is a multi-discipline body at the general officer/senior executive service-level, chartered to meet at least semi annually to improve doctrine, policy, tactics, techniques and procedures for FP operations. This structure may be mirrored at the MAJCOM level.

2.13. Standard 13: AT Physical Security Measures.

2.13.1. Principles of AFI 31-101, DoD 5200.08-R, *Physical Security Program*, and Antiterrorism Handbook, are applied and fully integrated into AT plans to ensure employment of a holistic security system to counter terrorist capabilities. Well-designed physical security measures are multi-layered and include the integration and synchronization of the essential elements of detection, assessment, delay or denial, communication and response. The development of comprehensive physical security measures requires the integration of facilities, physical security equipment, trained personnel, biometrics entry control equipment, procedures oriented at a minimum in support of perimeter and area

security, access and egress control, protection against CBRNE attacks (including those using the postal system and food/water supplies), HRP protection, barrier plans, and facility standoff distances.

2.13.2. Tenant unit security plans and measures, to include those of non-USAF elements, shall be coordinated and integrated into the host installation IDP and referenced in the AT plan.

2.13.3. Security Forces employing Explosive Detection Equipment (EDE) must be trained on employment of EDE and ensure sufficient consumables are maintained to allow random or spot inspections.

2.13.3.1. The Navy has been designated as DoD lead for the Explosive Detection Equipment RDT&E Program. Reports can be accessed at: **https://www.us.army.mil/suite/folder/9892268**. Must register for an AKO account first, then ask for privileges to folder.

2.13.4. Ensure installation access control points and associated barrier plans are constructed and operated IAW the Antiterrorism Handbook; UFC 4-022-01, *Security Engineering: Entry Control Facility/Access Control Points*; DTM 09-012, *Interim Policy Guidance for DoD Physical Access Control;* and AFI 31-113, *Installation Perimeter Access Control*.

2.13.4.1. Installations will enforce proper standoff by employing UFC 4-010-01 and Antiterrorism Handbook recommended barriers. Where there is a threat from a moving vehicle and continuous operation is mission essential, or the occupants cannot be evacuated, the type of barrier chosen must prevent a moving vehicle from encroaching into the standoff area.

2.13.4.2. Barrier plans also identify responsibility for executing the barrier plan and establish timelines for implementation.

2.14. Standard 14: Random Antiterrorism Measures (RAM).

2.14.1. The RAM program is developed and implemented as an integral component of the overall AT program and guided by the principles outlined in the Antiterrorism Handbook. To maximize the effectiveness and deterrence value, RAMs should be developed to counter risk from threats identified in the installation Threat Assessment, and implemented without a set pattern, either in terms of the measure selected, time, place or other variables. Lessons learned have highlighted unpredictability in security activities as one of the best and most cost effective deterrents available to a commander. Randomly changing AT measures enable integrated defenses to appear formidable and prevent threats from easily discerning and predicting patterns or routines that are vulnerable to attack. RAMs, at a minimum, shall consist of the random implementation of higher FPCON measures, to include MAJCOM or locally developed site-specific measures. Random use of other security measures, to include technologies, should be used to supplement FPCON measures. The RAM program shall be included in AT plans.

2.14.2. When developing and implementing an effective installation RAM program:

2.14.2.1. Include tenant units and organizations.

2.14.2.2. Implement daily RAMs to include weekends and holidays. The frequency will be increased as the threat increases. At least three RAMs chosen from higher FPCONs are required daily.

2.14.2.3. Consider implementing RAMs to mitigate and reduce risk for existing vulnerabilities.

2.14.2.4. RAM implementation shall be compatible and coordinated with ongoing law enforcement or CI surveillance detection and ID measures. When random vehicle inspections (RVI) are employed as a RAM, ensure pre-coordination with the installation legal office. Follow existing law enforcement rules when employing RVIs as a RAM.

2.14.2.5. Consider methods to make RAMs visible in order to confuse or expose enemy surveillance attempts and preoperational planning.

2.14.2.6. Make efforts to include local, State, Federal and host nation law enforcement patrols and first responders, as appropriate.

2.14.2.7. Implement RAMs installation-wide or focused on facilities or functions identified as potential targets. When implementing facility-specific RAMs, consider the possibility increased security on a particular building may signal its importance.

2.14.2.8. Installation RAM implementation efforts shall be monitored, tracked and analyzed by the installation ATO. Effectiveness of RAMs should be measured by the ATO and analyzed by the TWG.

2.15. Standard 15: AT Measures for AF Off-Installation Facilities, Housing and Activities.

2.15.1. Installations shall include specific AT measures for AF-owned or leased off-installation facilities, housing, transportation services, daycare centers, and other activities used by or involving a mass-gathering of DoD personnel and/or their dependent family members in their overall AT programs. At locations where there are multiple DoD components or locations, AT measures shall be coordinated with the designated senior DoD Component with AT responsibility.

2.15.2. Risk mitigation measures for AF-owned or leased off-installation facilities, housing and activities shall include, but are not limited to: emergency notification and recall procedures, guidance for selection of off-installation housing, temporary billeting and other facility use (including compliance with UFC 4-010-01 for leased, newly-constructed and expeditionary buildings), physical security measures, CBRNE defensive measures and shelter-in-place (ensure consistency and interoperability with CEMP 10-2), and relocation and evacuation procedures.

2.15.3. Develop appropriate support agreements (e.g., MOU, MOA, MAA) with appropriate federal, state, local, or tribal/host nation authorities to coordinate security measures, response capabilities, and assistance requirements.

2.15.3.1. Ensure such agreements are reviewed annually by the OPR, ATWG and JA for currency and executability. They should be exercised annually and all parties to the agreement should participate in at least one exercise annually.

2.15.3.2. It is the specific responsibility of the support agreement OPR to coordinate the support agreement and ensure one copy is filed with the installation office of primary responsibility for support agreements.

2.16. Standard 16: AT Measures for High-Risk Personnel (HRP).

2.16.1. Develop AT measures pursuant to the principles outlined in DoD O-2000.12-H, DoDI O-2000.22, and AFI 71-101, Volume 2, *Protective Service Matters*, for personnel designated as HRP.

2.16.1.1. SAF/IGX is the HAF focal point for policy development and coordination with the OASD for Special Operations and Low-Intensity Conflict and Interdependent Capabilities (OASD (SO/LIC&IC)) to implement DoDI O-2000.22.

2.16.1.2. AFOSI is designated as the AF lead Protection Providing Organization (PPO) and is the AF lead for Protective Service Details (PSD) and PSVAs IAW AFI 71-101, Volume 2.

2.16.2. Designation of positions as High-Risk Billets (HRB) and HRP shall be IAW DoDI O-2000.22 and AFI 71-101, Volume 2.

2.16.2.1. SAF/IGX shall staff nomination packages for the Secretary of the Air Force (SecAF), who will make the decision to nominate AF officials to the Office of the Secretary of Defense (OSD).

2.16.2.2. SAF/AA shall staff nomination packages for the AF Top-4, as appropriate.

2.16.2.3. Nomination packages shall be staffed through the appropriate MAJCOM or AF Component to a GCC.

2.16.3. AFOSI will complete a PSVA for each person occupying an HRB who is nominated for HRP IAW DoDI O-2000.22 and AFI 71-101, Volume 2. PSVAs will be initiated within 90 days of an individual's assignment to a HRB and nomination for HRP. PSVAs will be revalidated annually and updated if the TTL changes, but no less than every 3 years.

2.16.4. HRP and family members, as appropriate, shall complete appropriate AFOSI-sponsored HRP training (i.e., personal protection, evasive driving, AT awareness and hostage survival); shall be properly cleared for assignment to positions, facilities or countries requiring such protection; and shall be thoroughly indoctrinated on the duties and responsibilities of protective service personnel.

2.16.5. HRP designees and their family members shall be familiar with treaty, statutory, policy, regulatory and local constraints on the application of supplemental security measures for certain high-ranking DoD officials who are provided additional protection due to their position.

2.16.6. HRP security measures shall be reviewed within 60 days of changes to the TTL for the affected country and HRP.

2.16.7. The provisions of AFI 23-302, *Vehicle Management*, shall be complied with for the acquisition and use of non-tactical armored vehicles.

2.16.8. Use UFC 4-010-03, *Physical Security Measure for High-Risk Personnel*, in conjunction with a PSVA when available. When a PSVA is not available, this document may

also be used as selection criteria for a HRP residence or office. UFC 4-010-03 provides planning and design guidance for construction, renovation, and leases associated with the primary residence or office of a HRP. However, these criteria are not intended for HRP protection in combat zones and in areas where contingency or expeditionary operations are underway.

2.17. Standard 17: AT Construction and Building Considerations.

2.17.1. AT construction standards apply to all DoD Components, to all DoD inhabited buildings, billeting, and high occupancy family housing and to all DoD expeditionary and temporary structures in accordance with UFC 4-010-01. Attachment 6 provides guidance on requesting a UFC AT standards deviation.

2.17.2. Refer to UFC 4-010-01, AFPD 31-1, AFI 31-101, AFI 65-601, Volume 1, *Budget Guidance and Procedures*, and AFH 32-1084, *Facility Requirements*, for additional information. Proper facility project planning, programming and design must be done in concert with the ATO, installation intelligence and security personnel to adequately address site specific threats.

2.17.3. The installation commander or the senior Civil Engineer on the commander's behalf will certify that new facilities, or renovation projects where the UFC has been triggered, comply with UFC AT standards.

2.17.4. Engineering staff will work with the ATO from design inception to project completion, to ensure AT requirements are met. The ATO shall be part of the coordination process prior to certification.

2.17.5. Ensure the A7C (CE) and ATO develop a prioritized list of risk mitigation measures (reference DoD O-2000.12-H, UFCs and AFI 31-101) for use by site selection teams. These criteria shall be used to determine if facilities either currently occupied or being considered for occupancy provide adequate protection for DoD personnel against the effects of a terrorist attack. Circumstances may require the movement of DoD personnel or assets to facilities the U.S. Government had not previously used or surveyed. AT Standards shall be a key consideration in evaluating the suitability of facilities that were previously not used or surveyed.

2.17.6. The A7C (CE) will ensure at least one engineer at each installation has completed the Security Engineering and Design Course to review, document and track construction projects for compliance with UFCs and AT Standards. Take into consideration retention and competence of personnel. The U.S. Army Corps of Engineers (USACE) security engineering course and the Naval Facilities Engineering Service Center (NFESC) Antiterrorism/Security Engineering Workshop fulfills this requirement.

2.18. Standard 18: AT Measures for Logistics and Other Contracting.

2.18.1. AT measures shall be incorporated into the logistics and contracting processes (requirements development, vendor selection, award, execution and evaluation) when the provisions of the contract or services provided affect the security of DoD elements, personnel, mission-essential cargo, equipment, assets or services. When commensurate with risk, consider AT performance/compliance as an evaluation factor for contract award (past

performance and proposed performance under the instant contract) and as a performance metric under the resultant contract.

2.18.2. All unescorted persons entering DoD installations, to include contractors, sub-contractors and laborers, delivery personnel and vendors, must have a valid purpose to enter, have their identity proofed and vetted, and be issued, or be in possession of, an authorized and valid access credential. Refer to AFI 31-101 and AFI 31-113. For OCONUS locations, Commanders will work with local and host nation authorities to identity proof and vet applicants to the greatest extent practical and lawful IAW established SOFA.

2.18.3. Site-specific risk mitigation measures shall be developed and implemented to maintain positive control of DoD contractor and sub-contractor access to and movement within installations, sensitive facilities and classified areas.

2.18.4. Site-specific risk mitigation measures shall be developed and implemented to screen contractor or sub-contractor transportation conveyances for explosive hazards before entry into or adjacent to areas with DoD personnel and mission-essential assets.

2.18.5. Contracts shall comply with the AT clauses of the DFARS.

2.18.6. Contracts shall incorporate Level I - AT Awareness Training requirements (Standard 25).

2.19. Standard 19: AT Measures for Critical Asset Security.

2.19.1. IAW AFI 31-101, risk management measures shall be developed to reduce the risk of loss to DoD assets assessed as critical in Standard 5, to include distributive information or computer-based systems and networks. Integrate these measures into overall AT program efforts.

2.19.2. AFOSI and the DFC will coordinate with appropriate local, State, and Federal or tribal/host nation authorities responsible for the security of non-DoD assets deemed essential to the functioning of DoD assets assessed as critical.

2.19.3. Criticality assessments should be coordinated with affected DCIP and Air Force CARM, and conducted IAW the principles in DoDD 3020.40, AFPD 10-24, and identify defense critical infrastructure and critical assets.

2.20. Standard 20: Terrorism Incident Response Measures.

2.20.1. Incident response measures shall be developed consistent with the principles outlined in DoD 5200.08-R, DoDI 6055.17, and AFI 10-2501 and referenced in the overall AT plan. These measures shall include procedures for determining the nature and scope of incident response (including incidents with a CBRNE component); procedures for coordinating security, fire, medical, hazardous material and other emergency responder capabilities; and steps to recover from the incident while continuing essential operations. Appropriate reference will be made in the AT plan referencing the CEMP 10-2 for emergency response procedures.

2.20.2. AF Components to a GCC or GCCs prepare incident response measures for their AOR. AFOSI and Force Protection Detachments should be included in contingency planning for in-transit units.

2.21. Standard 21: Terrorism Consequence Management Measures.

2.21.1. Consequence management, CBRNE and public health emergency preparedness, and emergency response measures are included in AT Plans to complement and support the overall AT plan and installation emergency management plans. For the AF these measures are found in the CEMP 10-2, MCRP, AT, or IDP. Related contents of other plans should be referenced in the AT plan. These measures shall focus on mitigating vulnerabilities of personnel, families, facilities and materiel to terrorist use of CBRNE weapons, as well as overall disaster planning and preparedness to respond to a terrorist attack. These measures shall include integration with DoD emergency responder guidelines provided in DoDI 6055.17, AFI 10-2501, and mass notification system standards under UFC 4-021-01, *Design and O&M: Mass Notification Systems*; establishment of medical surveillance systems consistent with DoDD 6490.02E, *Comprehensive Health Surveillance* and AFI 10-2604, *Disease Containment Planning*; deployment of CBRNE sensors and detectors; providing collective protection when available in High Threat Areas as defined in AFI 10-2501; and providing personal protective equipment (PPE) or individual protective equipment (IPE) in the following priority and IAW AFI 10-2501:

2.21.1.1. First Responders and Emergency Responders. Personnel responding to known or suspected CBRNE hazards, as determined by incident commander, shall be provided protection needed to perform their duties in an unknown hazard environment. Responders should use the maximum possible protection until determined otherwise by competent authority.

2.21.1.2. Critical Personnel. Personnel deemed essential to the performance of critical military missions (whether military, civilian, contractor, host nation personnel or third country nationals), such as critical personnel assigned to mission essential functions (MEFs) described in AFI 10-208, *Continuity of Operations (COOP) Program*, shall be provided an appropriate level of protection to support continuity of those critical military missions. Since critical missions should be continued without interruption, collective or individual protection may be necessary to sustain them.

2.21.1.3. Essential Personnel. Personnel deemed essential to the performance of essential military operations (whether military, civilian, contractor, host nation personnel or third country nationals) shall be provided an appropriate level of protection to support continuity for those essential military operations. Since essential operations may be interrupted for relatively short periods (e.g., hours to days), appropriate protection may be necessary to sustain essential operations (i.e., escape, survive and restore essential operations).

2.21.1.4. Other Personnel. For all other persons not in the above categories, the objective will be to provide the procedures or protection necessary to safely survive an incident, e.g., shelter-in-place or evacuation procedures may fulfill this requirement.

2.21.1.5. Included as part of the above categories are those who work or live on DoD installations worldwide, family members authorized overseas and DoD contractors if designated in contract agreements and designated as essential to perform critical DoD missions. The contract Statement of Work or Performance Work Statement must specify if PPE will be government or contractor provided.

2.21.2. Site-specific C-CBRN preparedness and emergency response measures are developed and coordinated through the Emergency Management Flight and base medical personnel. These measures are implemented and synchronized with a corresponding FPCON measure for CBRNE-specific threats.

2.21.3. Support agreements (i.e., MOU, MOA, MAA) or other similarly constructed protocols will be established with the appropriate local, State, Federal or tribal/host nation authorities to support AT plan execution and augment incident response and post-incident consequence management activities.

2.21.4. The installation shall maintain mass warning and notification capabilities to warn all personnel immediately, but not longer than 10 minutes after incident notification and verification. The mass warning and notification must give response direction using intelligible voice communication, visible signals, text, text messaging, computer notification, tactile, or other communication methods.

2.21.5. Installation public health emergency response measures that are synchronized with FPCON levels shall be developed and implemented.

2.22. Standard 22: Force Protection Condition (FPCON) Measures.

2.22.1. The GCC is responsible for establishing the baseline FPCON for their AOR and procedures to ensure that FPCON measures are uniformly disseminated and implemented. The AF Component to the GCC is typically delegated to manage this task for the GCC. See Attachment 2 for a detailed listing of FPCON measures.

2.22.2. Installation commanders with AT responsibility and higher shall:

2.22.2.1. Determine an appropriate FPCON level for those personnel and assets for which they have AT responsibility. Subordinate commanders (to include GSUs and elements ‘off-site’) may raise a higher-level commander’s FPCON level, but they shall not lower the FPCON level without the higher-level commander’s written concurrence.

2.22.2.2. Classify site-specific AT measures and physical security actions, linked to a FPCON as “CONFIDENTIAL.” When separated from the AT plan, specific AT measures linked to a FPCON and site-specific FPCON levels may be downgraded to ”FOR OFFICIAL USE ONLY,” IAW DoD 5200.1-R, *Information Security Program*.

2.22.2.3. Notify their next higher level commander of any FPCON measures the installation is unable to fully implement or if it does not apply. The notification will include rationale, corrective action or mitigation, ECD for full implementation, and installation OPR.

2.22.2.4. Establish a review mechanism to ensure locally changed FPCON levels are commensurate with changing threats and the principles of risk management. This is essential because implementation of FPCON measures at elevated FPCON levels for an extended duration can be counterproductive to effective security and overall mission accomplishment. In some circumstances, based upon local conditions and the threat environment, commanders should consider requesting HHQ approval to implement a lower-level FPCON and supplement with other local security measures and RAMs as an effective alternative to executing the higher-level FPCON measures.

2.22.2.5. Develop and implement site-specific FPCON measures for AF installations and separate facilities to supplement the FPCON measures and actions enumerated for each FPCON level. In addition to establishing procedures for raising FPCON levels, ensure procedures are developed for stepping back down from higher FPCONs. Consult GCC supplementary FPCON guidance for in-transit forces. The development of site-specific FPCON measures must permit sufficient time and space to determine hostile intent, while fully considering constraints imposed by standing rules of engagement in CJCSI 3121.01B, *Standing Rules of Engagement/Standing Rules For the Use of Force For U.S. Forces*, and rules of force under AFI 31-207, *Arming and Use of Force by Air Force Personnel*. Organic intelligence, CI and law enforcement resources, institutional knowledge of the area and comprehensive understanding of organic capabilities, supported by national and AOR assets, shall be leveraged in directing tailored FPCON measures to be implemented at specific sites.

2.23. Standard 23: AT Training and Exercises.

2.23.1. All elements of the AT program shall be integrated into training and exercises related to Force Protection. AT lessons learned and the AT risk assessment (derived from the IDRMP) should guide the focus of training and exercises to ensure activities are supported by relevant threat, vulnerability, and criticality information.

2.23.2. Elements of the AT plan shall be exercised annually and synchronized with other ID, EM, COOP and CARM program requirements. The installation shall coordinate with the installation EET to develop a comprehensive annual exercise program which provides for individual and collective AT proficiency training and realistic AT exercise scenarios. The AT focus of exercises will be on the identification of vulnerabilities and AT program shortfalls which could contribute to the risk of terrorist attack against DoD personnel and assets. Scenarios must, at a minimum, exercise terrorist threat assessment and planning, mitigation and response to a terrorist incident (to include AT-specific MOA/MOU/MAAs and participation by local support elements), and consequence management measures following a terrorist incident. Site-specific FPCON measures from current FPCON through FPCON CHARLIE must also be exercised annually at all AF installations and separate facilities.

2.23.3. AT exercise documentation shall be maintained for no less than two years by Installation EET. Identified exercise findings will be presented to the ATWG and tracked/managed by installation EET until corrected or closed. AT lessons learned must be incorporated into appropriate plans and programs and submitted into the Joint Lessons Learned Information System (JLLIS) at **https://www.jllis.mil**. AT training shall also be incorporated into pre-deployment training and exercises as required by the GCC. Pre-deployment AT training exercises should include terrorism scenarios specific to the deployed location and based on current enemy Tactics, Techniques, and Procedures. Refer to paragraph 2.7.2 for a list of AT threat planning scenarios to assist in exercise development. Units will ensure they allow for a local Table and Rule within their respective file plans to maintain this reference data for unit continuity and action as required.

2.24. Standard 24: Formal AT Training.

2.24.1. The AF's formal AT Training Program shall consist of: Level I - AT Awareness Training (Standard 25), Level II - ATO Training (Standard 26), Level III - Pre-Command AT

Training (Standard 27), Level IV - AT Executive Seminar (Standard 28), AOR-specific training (Standard 29) and HRP AT training (Standard 16).

2.24.2. AT training shall be integrated into training for all AF personnel as required by this Instruction and when deemed appropriate by Commanders with AT responsibility. A solid training foundation for all grades, skills and functional areas is essential to successful implementation and long term effectiveness of AT programs.

2.24.2.1. Unit commanders, through their training NCO or section, shall ensure that all assigned personnel complete appropriate formal AT training. Additional protection related courses (such as Security Engineering Design Course and Dynamics of International Terrorism) are encouraged. Individual training records shall be updated accordingly.

2.24.2.2. If personnel have not received formal AT training as required, training shall be provided as soon as possible. Units receiving untrained personnel (PCS or deployed) should report training deficiencies through the AF chain of command to the appropriate losing MAJCOM functional office. Report other Service training discrepancies through the appropriate AF Component to the GCC.

2.25. Standard 25: Level I - AT Awareness Training.

2.25.1. The objective of Level I - AT Awareness Training is to provide all AF personnel with requisite knowledge necessary to remain vigilant for possible terrorist actions and enable employment of the AT TTP as outlined in DoD O-2000.12-H.

2.25.2. Every AF Service member, civilian employee, and local national or third country national in a direct-hire status by the DoD, regardless of grade or position shall complete Level I - AT Awareness Training annually.

2.25.2.1. New accession AF military personnel are provided Level I - AT Awareness Training during initial accession training or general military subject training. This initial accession Level I - AT Awareness Training shall be provided by a qualified Level I Awareness Training Instructor.

2.25.2.2. Post-accession annual Level I - AT Awareness Training may be accomplished by either a Level I - qualified instructor, or by completing the "Force Protection" computer based training (CBT) course on the Advanced Distributed Learning System (ADLS) or the Defense Technical Information Center (DTIC) at **https://atlevel1.dtic.mil/at** for individuals without access to NIPR, possessing a CAC card, nor enrolled in DEERS. The ADLS "Force Protection" CBT does not meet Department of State (DoS) Chief of Mission (CoM) requirements for Level I - AT Awareness Training.

2.25.2.2.1. AF personnel being assigned to a location where they will be under the responsibility of the DoS CoM for force protection must receive Level I - AT Awareness refresher training from a Level I-qualified instructor.

2.25.2.2.2. Unit Training Managers track annual Level I - AT Awareness Training through the ADLS. If ADLS is not available or not applicable, Unit Training Managers will document AT Awareness Training on ancillary training records. Unit Training Managers will provide AT training status and statistics to their chain of

command or the ATO upon request. Unit Deployment Managers and FSS will confirm training is current prior to approving OCONUS deployment or PCS orders.

2.25.2.3. DoD contractors shall be provided AT information as required by DFAR, Section 252.225-7043. Level I - AT Awareness Training shall be offered to all DoD contractor employees in the terms and conditions of the contract. The ATWG should determine the best method for offering AT Awareness training to contractor employees.

2.25.3. Commanders will ensure dependent family members ages 14 years and older traveling OCONUS on official business (e.g., on an accompanied permanent change of station move) shall complete Level I - AT Awareness Training as part of their pre-departure requirements. FSS will confirm training is completed before issuing dependent travel orders. Commanders will also encourage dependent family members to complete Level I - AT Awareness Training before any personal travel such as leave to an OCONUS location or any area where the TTL is MODERATE or higher.

2.25.4. Level I - AT Awareness Training instructors must have completed an AF-approved Level II - ATO Training course as outlined in Standard 26 of this publication. ATOs will maintain appointment letters of qualified instructors. If a certified instructor is not available, as an interim solution, unit commanders in coordination with the ATO may certify and appoint qualified SMEs to conduct training. Qualified SMEs must have completed Level I - AT Awareness Training and the Level II Refresher CBT available on ADLS. Commanders must clearly describe the qualifications of the individual in the appointment letter to justify this method and explain why other options are not feasible.

2.25.5. The ADLS “Force Protection” course covering Level I - AT Awareness Training will be updated annually by HQ AFSFC/SFOZ.

2.25.6. The AF’s Level I - AT Awareness Training is built upon the minimum requirements outlined in DoDI 2000.16, Standard 25, Table E3.T2 which is supplemented with topics specific to AF training. The AF Level I - AT Awareness (Force Protection) CBT is based upon and incorporates the DoD-sponsored and certified computer based Level I - AT Awareness Training course. Table 2.2 below outlines the minimum required topics to be covered in AF Level I - AT Awareness Training.

Table 2.2. Level I - AT Awareness Training Requirements

AF Level I - AT Awareness Training shall include the following at a minimum:

- Introduction to Terrorism
  - Includes Terrorist Tactics and Operations, Understanding the Terrorist Threat, Terrorist Surveillance Techniques, and Historical Examples
  - Indicators of Potential Terrorist Activity
- Individual Protective Measures
  - Includes Employing Situation-Based Measures to Lower Personal Vulnerability
- Response to Threat Actions
  - Includes counter-intelligence measures and personal protective actions to mitigate and reduce vulnerability to Improvised Explosive Device attacks, Active Shooter, Kidnapping and Hostage Survival, CBRNE attacks, and other likely terrorist tactics
- Supporting Unit Security and the AT Program
  - Includes Terrorism Threat Levels and FPCONs, and Force Health Protection Measures
- Current training aids and resource hand-outs (i.e., Chairman of Joint Chiefs of Staff Guide 5260, *A Self Help Guide to Antiterrorism*, Chairman of Joint Chiefs of Staff Pocket Card 5260, *Antiterrorism Individual Protective Measures*, Eagle Eyes tri-fold, etc.) shall be made available by the installation ATO

2.26. Standard 26: Level II – ATO and ATR Training.

2.26.1. Each USAF installation and separate facility shall have a Level II certified ATO appointed in writing. Each unit, who is authorized manning is 299 or less, supporting the installation and separate facility shall have an ATR appointed in writing. Level II – ATO and ATR Training prepares and qualifies Installation ATOs and Unit-level ATRs to perform their duties as AT program advisors and coordinators. Level II training is separated into two distinct tracks to ensure appropriate focus for the respective roles of ATOs and ATRs.

2.26.1.1. Newly assigned ATOs and ATRs shall complete training within 180 days of appointment. Deploying ATOs will complete training prior to deployment in accordance with line remarks. Unit level ATRs unable to secure in-residence training will complete the AT Level II Refresher CBT (within 180 days) until they are able to attend an in-residence AT Level II course. For both ATOs and ATRs, Level II refresher training must be completed once every three years to maintain qualification. Refresher training may be accomplished by taking the "AT Level II Refresher" CBT available on ADLS or by attending a Military Department -approved Level II course either in residence or offered by an MTT.

2.26.2. Level II – ATO and ATR training course instructors should have at least two years of experience in the field of Antiterrorism and should seek to remain proficient and further their expertise by attending seminars and courses related to Antiterrorism such as Security Engineering Design and Dynamics of International Terrorism. Also consider coordinating with JSIVA/AFVAT to shadow teams during an assessment. At a minimum, Level II instructors will have completed the following qualification requirements and have task certifications documented in training records as appropriate:

2.26.2.1. Formal training from an AF instructor's course such as Principles of Instruction. Personnel may instruct students prior to completing an instructor's course if supervised by a certified instructor.

2.26.2.2. AF-approved Level II - ATO Training course.

2.26.2.3. CVAMP training.

2.26.3. Level II - ATO and ATR Training must reflect current information on terrorism and AT Program guidance. The course plan must also include measurable course objectives and evaluation methods to ensure student proficiency. The AF's Level II – ATO and ATR Training is built upon and supplements the minimum requirements outlined in DoDI 2000.16, Standard 26, Table E3.T3. Training will be developed and reviewed annually by the MAJCOM sponsoring the course. Required course topics for the AF's Level II - ATO and ATR Training are listed below in Table 2.3. MAJCOM-specific requirements may be added to the core curriculum. MAJCOM ATPMs shall submit Level II - ATO Training course plans to AFSFC/SFOZ for annual review/approval during the first quarter of each calendar year.

Table 2.3. Level II – ATO and ATR Training Requirements

1. ATO Training must include the following topics:
    a. Overview of AF Force Protection
    b. Introduction to DoD and AF AT Programs
        i. Review of Applicable Guidance and References
        ii. Roles and Responsibilities
    c. Overview of Domestic and International Terrorism
    d. Development of an AT Plan and Integrating Plans
    e. Coordination and Management of an Installation AT Program
    f. Working Groups Related to AT
    g. AT Considerations in MOA/MOU/MAA
    h. Terrorist Threat Assessment and Analysis
    i. Intelligence Support to Force Protection
    j. CVAMP User/Administrator Review
    k. Vulnerability Assessments and AT Program Reviews
    l. AF CARM
    m. Risk Management Process
    n. AT Training and Exercises
    o. Physical Security
    p. Resource Application
    q. SME Presentations
    r. "Hands-on" Training with AT Tools and Resources (to include CVAMP, ATEP, IDRMP, and eGuardian), if available

2. ATR Training must include the following topics:
    a. Overview of AF Force Protection
    b. Introduction to AF AT Program
        i. Review of Applicable Guidance and References
        ii. AT Roles and Responsibilities at an Installation
    c. ATR Support to Installation AT Program
    d. Development of a Unit AT Plan
    e. Managing a Unit AT Program
    f. Overview of Domestic and International Terrorism
    g. Working Groups
    h. Risk Management Process
    i. Introduction to CVAMP
    j. Vulnerability Assessments of Squadron and Individual Facilities
    k. Physical Security
    l. Resource Application
    m. SME Presentations

2.27. Standard 27: Level III - Pre-Command AT Training.

2.27.1. Level III - Pre-Command AT Training provides prospective squadron, group, and wing commanders and civilian equivalent positions with requisite knowledge to direct and supervise an AT Program.

2.27.2. Squadron, group and wing commanders and civilian leaders in equivalent positions with AT responsibility shall complete Level III - Pre-Command AT Training prior to assuming command.

2.27.3. MAJCOMs will ensure this training is provided to squadron commanders. Training may be conducted during MAJCOM Squadron Commander Orientation seminars or by other means determined by the MAJCOM. Group and wing commanders shall receive the training through group and wing commander pre-command courses. Follow-on training may be conducted at the installation-level as a refresher or supplement to briefings offered in commander courses.

2.27.3.1. MAJCOMs shall determine minimum instructor qualifications and select instructors for Level III - Pre-Command AT Training. Instructors should be Level II qualified, have experience in the field of Antiterrorism, be familiar with command considerations regarding AT programs, and be able to explain the relationship and integration of Force Protection programs. Installation ATOs may conduct Level III supplemental training at the installation level in coordination with MAJCOM ATPMs.

2.27.3.2. Level III - Pre-Command AT Training course plans/briefings shall be developed and approved by the MAJCOM. Training material shall be coordinated through HQ AFSFC/SFOZ and AF/A7SO to ensure information is current and accurate.

2.27.4. Level III - Pre-Command AT Training is built upon the requirements outlined in DoDI 2000.16, Standard 27, Table E3.T4. AF requirements listed in Table 2.4 below supplement DoD Standard 27. A minimum of one hour is recommended to sufficiently address required topics.

Table 2.4. Level III - Pre-Command AT Training Requirements

At a minimum, Level III - Pre-Command AT Training shall include the following topics:
- Overview of AF Force Protection
- Overview of AF AT Program
- Review of Applicable Guidance and References
- AT Roles and Responsibilities
- Elements of an AT Program
- Risk Management—Assessment of Threat, Criticality and Vulnerability, Assessment of Risk, and Mitigation of Risk
- Working Groups and the Development of AT Plans
- Creating and Supervising a Sustainable AT Program
- Overview of CVAMP and the Role of a Commander
- Executing Resourcing Responsibilities

2.28. Standard 28: Level IV - AT Executive Seminar.

2.28.1. The CJCS-sponsored Level IV - AT Executive Seminar provides DoD senior military and civilian executive leadership with requisite knowledge to enable development of AT program policies and facilitate oversight of AT programs at the operational and strategic levels.

2.28.2. Wing and group commanders and other command and staff officers in the grades O-6 through O-8 and civilian equivalent/senior executive service civilian employees may attend

the Level IV - AT Executive Seminar. Nomination requests for attendance are made through HQ USAF/DPO for USAF quotas, and COCOM J-34 or force protection offices for COCOM quotas.

2.28.3. The seminar is administered by the Joint Staff (J3, DD AT/HD, J34) and provides AT updates, briefings, panel discussion topics, and tabletop AT and Terrorist Consequence Management war games.

2.29. Standard 29: Area of Responsibility (AOR)-Specific Training for DoD Personnel and In-transit Forces. AF Commanders shall:

2.29.1. Ensure that personnel for whom they are responsible (including family members ages 14 years and older) who are being assigned permanently or temporarily, transiting through, or performing exercises or training in another GCC's AOR receive or participate in AT Awareness Training and Education programs developed by that GCC to orient all DoD personnel with AOR-specific information on AT protection. This AOR-specific information is in addition to annual Level I - AT Awareness Training and may be provided through multiple means including Combatant Command publications, messages, internet homepages, and the Department of Defense Foreign Clearance Guide.

2.29.2. Ensure that AF personnel (including family members ages 14 years and older) departing to another GCC's AOR complete the gaining Combatant Commander's AOR-specific AT Awareness Training and Education requirements within three months of a permanent change of station.

2.29.3. Ensure their deploying in-transit forces, units and individuals receive GCC-provided detailed threat information covering transit routes and sites that will be visited by the deploying unit or individuals. Such information shall include focused information on potential terrorist threats (e.g., tailored production and analysis) and guidance on the development of AT protection risk mitigation measures to aid in the development of tailored AT planning. Similar tailored information shall also be received from the GCC and provided to intra-theater transiting units and individuals.

2.30. Standard 30: AT Resource Application.

2.30.1. Commanders shall assess risk against the standard and apply mitigation measures. Where the resulting risk is still deemed too great, the countermeasure requirement shall be elevated using the PPB&E process. Where applicable and IAW the MOU between the Department of State (DOS) and the DoD, Overseas Security Support, coordination will be made through MAJCOMs or AF Components to GCCs with the appropriate GCC to ensure that resource requirements for AT programs are identified and programmed. See Attachment 4 for more information on AT resourcing.

2.30.2. For emergent or emergency AT requirements that could not reasonably have been anticipated or programmed, units shall submit CCIF requests to their owning MAJCOM. MAJCOMs will submit requests for CCIF to the AF Component to the GCC who will prioritize and submit to the GCC as specified in CJCSI 7401.1. Comply with GCC-established procedures and policies for CCIF submittals.

2.30.3. MAJCOMs will submit validated prioritized AT resource requests with compelling justification, including those submitted or considered for CCIF, to the AF Component to the

GCC for review and submission to the GCC which will review and submit to CJCS on an annual basis pursuant to current DoD Program Objective Memorandum (POM) guidance and timelines, using CVAMP.

2.30.4. Tenant units on AF installations and facilities shall coordinate and prioritize AT program and resource requirements according to PPB&E procedures with the host installation commander, applicable Military Department and appropriate GCC.

2.30.5. Antiterrorism PEC 28047F is the primary funding source for manpower authorizations, AT equipment, procurement, and the associated costs specifically identified and measurable to those resources and activities associated with the Air Force AT Program. AF/A7SX is the AF Program Element Monitor (PEM).

2.31. Standard 31: Comprehensive AT Program Review.

2.31.1. Comprehensive AT program reviews are conducted to evaluate the effectiveness and adequacy of AT program implementation. The evaluation shall include an assessment of the degree to which Air Force AT programs comply with the standards prescribed in this Instruction. AT program reviews shall evaluate all mandatory AT program elements (Standard 1) and assess the viability of AT plans (Standard 7) in view of local operational environment constraints and conditions. The DoD Antiterrorism Handbook provides procedures and recommendations to conduct comprehensive AT Program reviews. Other procedures include reviewing AT programs based on DoD, GCC, and AF VAT AT benchmarks.

2.31.2. Comprehensive AT program reviews shall be conducted at least annually by all commanders required to establish AT programs and may be conducted in conjunction with annual VAs.

2.31.3. Pre-deployment AT program reviews shall be conducted to ensure that deploying units have viable AT programs and executable AT plans for transit to, from, and during operations or training exercises in the deployed AOR IAW GCC's AT guidance.

2.31.4. A comprehensive AT program review shall be conducted whenever there are significant changes in threat, vulnerabilities or asset criticality.

2.31.5. MAJCOMs shall ensure subordinate commands undergo a HHQ AT program review at least once every 3 years. The ultimate outcome of triennial AT program reviews is the identification of AT program deficiencies that may be exploited by terrorists. AT program review teams should provide realistic solutions aimed at improving AT program implementation and risk mitigation strategies.

2.31.5.1. Triennial AT program reviews conducted in conjunction with a HHQ VAs or JSIVAs satisfy the requirement for an annual AT program review.

2.31.5.2. In addition to providing an assessment of compliance with the AT Standards, a HHQ VA or JSIVA shall assess and evaluate the viability of a headquarter's AT policies, subordinate AT program implementation, the methodology for addressing resource shortfalls, inter-organization coordination and synchronization of AT program elements.

2.31.6. Tenant commands and units located on AF installations shall be included in comprehensive AT program reviews.

2.32. Standard 32: AT Program Review Teams.

2.32.1. AT program review assessment team guidelines shall be modeled upon the DTRA AT VA Team Guidelines and include, at a minimum, compliance with the standards prescribed in this Instruction, accepted TTPs, and AT best practices.

2.32.2. A sufficient number of AT program review teams shall be resourced to execute the program review assessment requirements of the AF and to ensure AT program review teams are comprised of individuals with sufficient functional expertise to assess and evaluate satisfactorily the effectiveness and adequacy of AT Program implementation at the level for which the AT Program review is being conducted (headquarters, command, installation, unit, activity, etc.).

Chapter 3 (Added-30SW)

DESCRIPTION OF 30 SW VISUAL AIDS (VA)

3.1. (Added-30SW) All 30 SW FPCON VAs are to be obtained from Air Force e-Publishing at www.e-publishing.af.mil. They are to be printed using landscape orientation. The enclosed attachments are for representational use only and the size, color, layout, and fonts may vary from the actual VA posted at the listed web site above.

3.2. (Added-30SW) The 30 SW FPCON VA signs- are numbered 30 SWVA 10-1, 10-1A, 10-2, 10-2A, 10-3, 10-3A, 10-4, 10-4A, and 10-5.

3.3. (Added-30SW) The 30 SW/CCH-, located at Bldg 10577, Room C-101, 606-6604, will provide details on procedures and materials to be used in printing the 30 SW FPCON VA. To the greatest extent possible, signs will be uniform and standardized throughout Vandenberg AFB.

3.3.1. **(Added-30SW)** Proper materials can be obtained through the base supply store or Service Store in Bldg 5500. For those who do not have access to this facility (contractors), please acquire similar materials to produce the 30 SW FPCON VA signs.

Chapter 4 (Added-30SW)

GENERAL GUIDANCE FOR THE USE OF 30 SWVA 10-1 THROUGH 30 SWVA 10-5A, FPCON SIGNS

4.1. (Added-30SW) The proper 30 SW FPCON VA sign- shall be displayed at all times according to the current local FPCON level as a means to notify VAFB personnel of the current level of terrorist threat. While no longer required by the DoD or Service, the 30 SW/CC has deemed the use of local FPCON signs important in keeping personnel advised and safe.

4.1.1. **(Added-30SW)** During installation exercises it is necessary to display the current real world FPCON sign and the applicable exercise FPCON sign concurrently. Upon termination of the installation exercise, display only the current real world FPCON sign.

4.1.2. **(Added-30SW)** The 30 SW/CC has approved the use of an alternate aesthetic FPCON sign in lieu of the laminated paper visual aids. These plastic signs with slide in FPCON level indicators are intended to be used on the primary entrances to key facilities, as designated by group or unit commanders, and can be purchased at the unit's expense by contacting 30th Force Support Squadron Arts & Crafts Center (Bldg 11193) at 606-6438.

4.2. (Added-30SW) All facilities- that are open and in use must conspicuously display the current FPCON sign(s) on or adjacent to each entrance door in use.

4.2.1. **(Added-30SW)** Entrance doors which are not in use (locked or blocked) do not require an FPCON sign. Locked doors which are in use by personnel with keys should display the proper signs.

4.2.2. **(Added-30SW)** Update facility FPCON signs as soon as the local FPCON level changes.

4.2.2.1. **(Added-30SW)** Facilities that are closed do not need to update FPCON signs until the facility reopens. Immediately update the facility FPCON signs upon opening the facility and prior to arrival of personnel.

4.3. (Added-30SW) Consider storing FPCON signs in a holder adjacent to doors. If a sign discrepancy is noted, any facility occupant will be able to update the signs. This will assist the facility manager in updating the signs and increases the likelihood of accurate sign placement. Inform all facility occupants of the need to assist in keeping doors updated with current signs.

Chapter 5 (Added-30SW)

USE OF THE 30 SWVA 10-1 THROUGH 30 SWVA 10-5, FPCON SIGNS

5.1. (Added-30SW) Use of the FPCON Normal Real-World Visual Aid, 30 SWVA 10-5: The FPCON Normal Real-World visual aid shall be displayed at all times when the local VAFB FPCON is set to FPCON Normal.

5.2. (Added-30SW) Use of the FPCON Alpha Real-World Visual Aid, 30 SWVA 10-1: The FPCON Alpha Real-World visual aid shall be displayed at all times when the local VAFB FPCON is set to FPCON Alpha.

5.3. (Added-30SW) Use of the FPCON Alpha Exercise Visual Aid, 30 SWVA 10-1A: The FPCON Alpha Exercise visual aid shall be displayed at all times during installation exercises when the local VAFB Exercise FPCON level is set to FPCON Alpha. Ensure the real-world FPCON visual aid is concurrently displayed.

5.4. (Added-30SW) Use of the FPCON Bravo Real-World Visual Aid, 30 SWVA 10-2: The FPCON Bravo Real-World visual aid shall be displayed at all times when the local VAFB FPCON is set to FPCON Bravo.

5.5. (Added-30SW) Use of the FPCON Bravo Exercise Visual Aid, 30 SWVA 10-2A: The FPCON Bravo Exercise visual aid shall be displayed at all times during installation exercises when the local VAFB Exercise FPCON level is set to FPCON Bravo. Ensure the real-world FPCON sign is concurrently displayed.

5.6. (Added-30SW) Use of the FPCON Charlie Real-World Visual Aid, 30 SWVA 10-3: The FPCON Charlie Real-World visual aid shall be displayed at all times when the local VAFB FPCON is set to FPCON Charlie.

5.7. (Added-30SW) Use of the FPCON Charlie Exercise Visual Aid, 30 SWVA 10-3A: The FPCON Charlie Exercise visual aid shall be displayed at all times during installation exercises when the local VAFB Exercise FPCON level is set to FPCON Charlie. Ensure the real-world FPCON sign is concurrently displayed.

5.8. (Added-30SW) Use of the FPCON Delta Real-World Visual Aid, 30 SWVA 10-4: The FPCON Delta Real-World visual aid shall be displayed at all times when the local VAFB FPCON is set to FPCON Delta.

5.9. (Added-30SW) Use of the FPCON Delta Exercise Visual Aid, 30 SWVA 10-4A: The FPCON Delta Exercise visual aid shall be displayed at all times during installation exercises when the local VAFB Exercise FPCON level is set to FPCON Delta. Ensure the real-world FPCON sign is concurrently displayed.

Chapter 6 (Added-30SW)

USE OF 30 SWVA 10-6 THROUGH 30 SWVA 10-9, ANTITERRORISM VISUAL AIDS

6.1. (Added-30SW) Four additional 30 SW AT VAs are available. They are numbered 30 SWVA 10-6, ***Threat Awareness Memory Jogger***, 30 SWVA 10-7, ***Suspicious Package/Letter/Unattended Item***, 30 SWVA 10-8, S***uspicious Powders or Substances***, and 30 SWVA 10-9, ***Bomb Threats***. These VAs provide information necessary to protect VAFB personnel, property, and resources. All personnel should receive initial/periodic training and be familiar with the informational content of these VAs.

6.2. (Added-30SW) Use of the Antiterrorism Memory Jogger Card, 30 SWVA 10-6: The Antiterrorism Memory Jogger provides personal protective measures and antiterrorism information. The card can be printed and carried on individuals or posted on unit/agency bulletin boards.

6.3. (Added-30SW) Use of the Suspicious Package/Letter/Unattended items Visual Aid, 30 SWVA 10-7: This VA provides information on how to detect, react to, and report suspicious packages, letters or unattended items. The VA should be posted within unit/agency mail rooms, mail reception points, and on unit/agency bulletin boards.

6.4. (Added-30SW) Use of the Suspicious Powder or Substance Visual Aid, 30 SWVA 10-8: This VA provides information on how to detect, react to, and report suspicious powder or substances. The VA should be posted within unit/agency mail rooms, mail reception points, and on unit/agency bulletin boards.

6.5. (Added-30SW) Use of the Bomb Threats Visual Aid, 30 SWVA 10-9: This VA provides information on how to detect, react to, and report bomb threats. The VA should be posted within unit/agency bulletin boards.

BURTON M. FIELD, Lt Gen, USAF
DCS/Operations, Plans & Requirements

(30SW)

NINA M. ARMAGNO, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFDD 3-10, Force Protection, 28 July 2011

AFDD 4-0, Combat Support, incorporating Change 2, 28 July 2011

AFPD 10-2, Readiness, 30 October 2006

AFPD 10-24, Air Force Critical Infrastructure Program (CIP), 28 April 2006

AFPD 10-25, Emergency Management, 26 September 2007

AFPD 10-26, Counter-Chemical, Biological, Radiological and Nuclear Operations, 26 September 2007

AFPD 10-39, Safeguarding Biological Select Agents and Toxins, 19 August 2011

AFPD 14-2, Intelligence Rules and Procedures, 29 November 2007

AFPD 31-1, Integrated Defense, 28 October 2011

AFPD 71-1, Criminal Investigations and Counterintelligence, 6 January 2010

AFI 10-206, Operational Reporting, 6 September 2011

AFI 10-208, Continuity of Operations (COOP) Program, 15 December 2011

AFI 10-246, Food and Water Protection Program, 4 December 2004

AFI 10-2501, Air Force Emergency Management (EM) Program, Planning and Operations, 24 January 2007 (AFGM4, 27 January 2012)

AFI 10-2603, Emergency Health Powers on Air Force Installations, 13 October 2010

AFI 10-2604, Disease Containment Planning, 3 September 2010

AFI 14-104, Oversight of Intelligence Activities, 16 April 2007

AFI 14-119, Intelligence Support to Force Protection (FP), 15 August 2007

AFI 23-302, Vehicle Management, 29 October 2007

AFI 31-101, Integrated Defense (FOUO), 8 October 2010

AFI 31-207, Arming and Use of Force by Air Force Personnel, 29 January 2009

AFI 31-113, Installation Perimeter Access Control, 26 January 2012

AFI 38-101, Air Force Organization, 16 March 2011

AFI 38-201, Management of Manpower Requirements and Authorizations, 26 September 2011

AFI 65-601, Volume 1, Budget Guidance and Procedures, 3 March 2005

AFI 71-101, Volume 1, Criminal Investigation Program, 8 April 2011

AFI 71-101, Volume 2, Protective Service Matters, 17 May 2011

AFI 71-101, Volume 4, Counterintelligence, 8 November 2011

AFI 90-201, Inspector General Activities, 23 March 2012

AFH 10-2401, Vehicle Bomb Mitigation Guide (FOUO), 1 September 2006

AFH 32-1084, Facility Requirements, 1 September 1996

AFMAN 33-363, Management of Records, 1 March 2008

AFMAN 10-2503, Operations in a Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive (CBRNE) Environment, 7 July 2011

AFMAN 33-363, *Management of Records*, 1 March 2008

AFPAM 14-118, Predictive Battlespace Awareness: Air and Space Intelligence Preparation of the Operational Environment, 10 March 2008

CJCSI 3121.01B, Standing Rules of Engagement/Standing Rules For the Use of Force For U.S. Forces (available on SIPR at **www.js.smil.mil/masterfile/sfsimd/jel/index.htm**), 18 June 2008

CJCSI 5261.01F, Combating Terrorism Readiness Initiative Fund, 13 December 2010

CJCSI 7401.1, Combatant Commander Initiative Fund, 1 July 2009

CJCS Guide 5260, Antiterrorism Personal Protection Guide: A Self-Help Guide to Antiterrorism, 1 September 2010

CJCS Pocket Card 5260, Antiterrorism Individual Protective Measures, 1 October 2001

DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 1 July 2010

DoDD 4500.54E, DoD Foreign Clearance Program (FCP), 28 December 2009

DoDD 6490.02E, Comprehensive Health Surveillance, incorporating Change 1, 24 August 2009

DoDI 2000.16, DoD Antiterrorism (AT) Standards, incorporating Change 2, 8 December 2006

DoDI 2000.12, DoD Antiterrorism (AT) Program, 1 March 2012

DoDI O-2000.22, Designation and Physical Protection of DoD High-Risk Personnel (HRP), 22 January 2008

DoDI 2000.26, Suspicious Activity Reporting, 1 November 2011

DoDI 3020.45, Defense Critical Infrastructure Program (DCIP) Management, 21 April 2008

DoDI 5210.89_AFI 10-3901, Minimum Security Standards for Safeguarding Biological Select Agents and Toxins, 22 June 2010

DoDI 5240.18, Counterintelligence (CI) Analysis and Production, 4 December 2009

DoDI 6055.17, DoD Installation Emergency Management (IEM) Program, incorporating Change 1, 19 November 2010

DoD O-2000.12-H, DoD Antiterrorism Handbook, 1 February 2004

DoD 5200.1-R, Information Security Program, 14 January 1997

DoD 5200.08-R, Physical Security Program, 9 April 2007

DoD 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons, 1 December 1982

DoDM 3020.45, Volume 1, Defense Critical Infrastructure Program (DCIP): DoD Mission-Based Critical Asset Identification Process (CAIP), 24 October 2008

DoDM 3020.45, Volume 5, Defense Critical Infrastructure Program (DCIP): Execution Timeline, 24 May 2010

DTM 10-018, Law Enforcement Suspicious Activity Reporting, 1 October 2010

JP 1-02, Department of Defense Dictionary of Military and Associated Terms, 30 May 2008

UFC 4-010-01, DoD Minimum Antiterrorism Standards for Buildings, 8 October 2003

UFC 4-010-02, DoD Minimum Antiterrorism Standoff Distances for Buildings, 8 October 2003

UFC 4-010-03, Security Engineering: Physical Security Measures for High-Risk Personnel, 8 February 2011

UFC-4-020-01, DOD Security Engineering Facilities Planning Manual, 11 September 2008

UFC 4-021-01, Design and O&M: Mass Notification Systems, 9 April 2008

UFC 4-022-01, Security Engineering: Entry Control Facility/Access Control Points, 25 May 2005

Defense Federal Acquisition Regulation Supplement (DFARS), 20 October 2008

DoD Antiterrorism Vulnerability Assessment Benchmarks, 5 January 2011

Defense Threat Reduction Agency (DTRA) Security Classification Guide (JSIVA), 1 February 2010

Presidential Policy Directive (PPD) 8, National Preparedness, 30 March 2011

Unified Command Plan, 17 December 2008

Adopted Forms

AF Form 847, Recommendation for Change of Publication

AF Form 116, Request For Deviation From Security Criteria

Abbreviations and Acronyms

AA&E—Arms Ammunition and Explosives

ACES—Automated Civil Engineering System

ADLS—Advanced Distributed Learning System

AF CARM—Air Force Critical Asset Risk Management

AF/A1—Deputy Chief of Staff of the Air Force, Manpower, Personnel and Services

AF/JA—The Judge Advocate General of the Air Force

AF/SE—Air Force Safety

AF/SG—Surgeon General

AFCESA—Air Force Civil Engineer Support Agency

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force Policy Directive

AFR—Air Force Reserve

AFSFC—Air Force Security Forces Center

AFTTP—Air Force Tactics, Techniques and Procedures

AFVAT—Air Force Vulnerability Assessment Team

ANG—Air National Guard

AOR—Area of Responsibility

AT—Antiterrorism

ATEC—Antiterrorism Executive Committee

ATO—Antiterrorism Officer

ATPM—Antiterrorism Program Manager

ATR—Antiterrorism Representative

ATWG—Antiterrorism Working Group

BSAT—Biological Select Agents and Toxins

CARA—Critical Asset Risk Assessment

CARM—Critical Asset Risk Management

C-CBRN—Counter-Chemical, Biological, Radiological and Nuclear

C-NAF—Component-Numbered Air Force

CBRN—Chemical, Biological, Radiological, Nuclear

CBRNE—Chemical, Biological, Radiological, Nuclear and high-yield Explosives

CBT—Computer Based Training

CbT—Combating Terrorism

CCIF—Combatant Commander's Initiative Fund

CCIR—Commander's Critical Information Requirements

CE—Civil Engineers

C&I—Communications and Information

CI—Counterintelligence

CJCS—Chairman of the Joint Chiefs of Staff

CJCSI—Chairman of the Joint Chiefs of Staff Instruction

COA—Course of Action

COCOM—Combatant Command

CoM—Chief of Mission

CEMP—Comprehensive Emergency Management Plan

CONOPS—Concept of Operations

CONUS—Continental United States

CRP—Contingency Response Plan

CTO—Counterthreat Operations

CVAMP—Core Vulnerability Assessment Management Program

DBIDS—Defense Biometric Identification System

DBT—Design Basis Threat

DCI—Defense Critical Infrastructure

DCIP—Defense Critical Infrastructure Program

DCP—Disease Containment Plan

DFARS—Defense Federal Acquisition Regulation Supplement

DFC—Defense Force Commander

DIA—Defense Intelligence Agency

DIRLAUTH—Direct liaison authorized

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DoS—Department of State

DRU—Direct Reporting Unit

DTA—Defense Threat Assessment

DTM—Directive Type Memorandum

DTRA—Defense Threat Reduction Agency

ECC—Emergency Control Center

ECD—Estimated Completion Date

EDE—Explosive Detection Equipment

EET—Exercise Evaluation Team

EM—Emergency Management

EMWG—Emergency Management Working Group

EOD—Explosive Ordnance Disposal

FHP—Force Health Protection

FOA—Field Operating Agency

FP—Force Protection

FPD—Force Protection Detachment

FPSG—Force Protection Steering Group

FPWG—Force Protection Working Group

FPCON—Force Protection Condition

FPI—Force Protection Intelligence

FSS—Force Support Squadron

FYDP—Future Years Defense Program

GCC—Geographic Combatant Commander

GSU—Geographically Separated Unit

HHA—Higher Headquarters Assessment

HAF—Headquarters Air Force

HN—Host Nation

HRB—High-Risk Billet

HRP—High-Risk Personnel

HSPD—Homeland Security Presidential Directive

ID—Integrated Defense

IDC—Integrated Defense Council

IDP—Integrated Defense Plan

IDRMP—Integrated Defense Risk Management Process

IDS—Intrusion Detection System

IDWG—Integrated Defense Working Group

IED—Improvised Explosive Device

IFC—Information Fusion Cell

INWS—Installation Notification and Warning System

IO—Intelligence Oversight

IPE—Individual Protective Equipment

JA—Judge Advocate

JAT—Joint Antiterrorism Guide

JLLIS—Joint Lessons Learned Information System

JNLWD—Joint Non-Lethal Weapons Directorate

JP—Joint Publication

JRO—CBRND —Joint Requirements Office for Chemical, Biological, Radiological and Nuclear Defense

JSIVA—Joint Staff Integrated Vulnerability Assessment

LFA—Lead Federal Agency

MAA—Mutual Aid Agreement

MAJCOM—Major Command

MCRP—Medical Contingency Response Plan

MEF—Mission Essential Function

MILCON—Military Construction

MOA—Memorandum of Agreement

MOU—Memorandum of Understanding

MTT—Mobile Training Team

NACI—National Agency Check with Inquiries

NAF—Numbered Air Force

NCIC—National Crime Information Center

NEO—Noncombatant Evacuation Operation

OASD—Office of the Assistant Secretary of Defense

OASD SO/LIC & IC—Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict and Interdependent Capabilities

OASD PA—Office of the Assistant Secretary of Defense for Public Affairs

OCONUS—Outside the Continental United States

OPCON—Operational Control

OPM—Office of Personnel Management

OPORD—Operation Order

OPR—Office of Primary Responsibility

OPSEC—Operations Security

OSD—Office of the Secretary of Defense

PA—Public Affairs

PE—Program Element

PEC—Program Element Code

PEM—Program Element Monitor

PHEO—Public Health Emergency Officer

PIR—Priority Intelligence Requirement

POA&M—Plan of Action and Milestone

POD—Port of Debarkation

POE—Port of Embarkation

POM—Program Objective Memorandum

PPB&E—Planning, Programming, Budgeting and Execution

PPO—Protection Providing Organization

PPE—Personal Protective Equipment

PSD—Protective Service Detail

PSEAG—Physical Security Equipment Action Group

PSVA—Personal Security Vulnerability Assessment

RAM—Random Antiterrorism Measure

RIEVC—Random Installation Entry/Exit Vehicle Check

RVI—Random Vehicle Inspection

SAF/AA—Secretary of the Air Force Administrative Assistant

SAF/FM—Assistant Secretary of the Air Force, Financial Management and Comptroller

SAF/IG—Secretary of Air Force Inspector General

SAF/PA—Secretary of Air Force Public Affairs

SAR/SIR—Suspicious Activity Report/Suspicious Incident Report

SecAF—Secretary of the Air Force

SCI—Sensitive Compartmentalized Information

SME—Subject Matter Expert

SOFA—Status of Forces Agreement

TACON—Tactical Control

TDY—Temporary Duty

TIC/TIM—Toxic Industrial Chemical/Toxic Industrial Material

TSWG—Technical Support Working Group

TTL—Terrorism Threat Level

TTP—Tactic, Technique and Procedure

TWG—Threat Working Group

UCP—Unified Command Plan

UFC—Unified Facilities Criteria

UMD—Unit Manning Document

UTC—Unit Type Code

VA—Vulnerability Assessment

VAPO—Vulnerability Assessment Protection Option

VAT—Vulnerability Assessment Team

VBIED—Vehicle Borne Improvised Explosive Device

WMD—Weapon of Mass Destruction

Terms

Active Defense—The employment of limited offensive action and counterattacks to deny a contested area or position to the enemy.

Air Force Emergency Management (EM) Program—The single, integrated Air Force program to coordinate and organize efforts to prepare for, prevent, respond to, recover from and mitigate the direct and indirect consequences of an emergency or attack. The primary missions of the Air Force EM program are to (1) save lives, (2) minimize the loss or degradation of resources and (3) continue, sustain and restore combat and combat support operational capability in an all-hazards physical threat environment at Air Force installations worldwide. The ancillary missions of the Air Force EM program are to support homeland defense and civil support operations and to provide support to civil and host nation authorities IAW DoD directives and through the appropriate Combatant Command. The Air Force EM program is managed by the Office of The Civil Engineer, AF/A7C.

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 and civilian forces.

Assessment—Analysis of the security, effectiveness and potential of an existing or planned intelligence activity (JP 1-02). [The evaluation of progress toward the creation of effects and the achievement of objectives and end state conditions.] Words in brackets apply only to the Air Force and are offered for clarity.

AT Awareness—Fundamental knowledge of both the terrorist threat and the measures to reduce personal vulnerability to terrorism.

AT Officer (ATO)—The principal military or civilian advisor charged with managing the AT program for the commander or DoD civilian exercising equivalent authority.

AT Planning—The process of developing specific guidance and execution-oriented instructions for subordinates. An AT plan contains command-specific guidance for the establishment of an AT program and the implementation of the AT Standards.

AT Program—One of several security-related programs that fall under the overarching combating terrorism and FP programs. The AT program is a collective, proactive effort focused on the prevention and detection of terrorist attacks against DoD personnel and their families, facilities, installations and infrastructure critical to mission accomplishment as well as the

preparation to defend against and planning for the response to the consequences of terrorist incidents. Although not elements of AT, plans for terrorism consequence management preparedness and response measures as well as plans for continuing essential military operations are important adjuncts to an effective AT program. The minimum elements of an AT program are AT risk management, planning, training and exercises, resource application and program reviews.

AT Program Review—The systematic assessment of the AT program against the AT Standards.

AT Resource Application—The process of applying risk management to vulnerabilities and where the resultant risk is not acceptable after applying mitigation measures, elevating the vulnerability with a resource request using the existing PPB&E system, the CCIF, the Physical Security Program and other funding mechanisms. Central to success in resource application is tracking and ensuring sufficient funding for identified AT program life-cycle costs and assessed shortfalls to mitigate risk associated with terrorist capabilities.

AT Risk Management—The process of systematically identifying, assessing and controlling risks arising from operational factors and making decisions that balance possible adverse outcomes with mission benefits. The end products of the AT program risk management process shall be the identification of DoD elements and personnel that are vulnerable to the identified threat attack means. From the assessment of risk based upon the three critical components of AT risk management (threat assessment, criticality assessment and vulnerability assessment), the commander must determine which DoD elements and personnel are at greatest risk and how best to employ given resources and FP measures to deter, mitigate or prepare for a terrorist incident.

AT Training and Exercises—The process of developing individual, leader and collective skills and of conducting comprehensive exercises to validate plans for AT incident response, consequence management and continuity of essential military operations.

Biological Select Agents and Toxins (BSAT)—Biological agents and toxins that present a high bioterrorism risk to national security and have the greatest potential for adverse public health impact with mass casualties of humans and/or animals or that pose a severe threat to plant health or to plant products. The lists are reviewed and updated by HHS/CDC and USDA/APHIS. Agents and toxins that are excluded in Title 42, Code of Federal Regulations, Part 73, and Title 7, Code of Federal Regulations, Part 331 are excluded as BSAT.

Combating Terrorism (CbT)—For the purposes of this Instruction, combating terrorism within the DoD encompasses all actions, including AT, counterterrorism, terrorism consequence management (preparation for and response to the consequences of a terrorist incident or event) and terrorism intelligence support (collection and dissemination of terrorism-related information), taken to oppose terrorism throughout the entire threat spectrum, including terrorist use of CBRNE.

Commander—Personnel assigned to command positions at all levels and the heads of the Defense Agencies and DoD Field Activities.

Commander's Critical Information Requirements (CCIR)—An information requirement identified by the commander as being critical to facilitating timely decision-making. The two key elements are friendly force information requirements (FFIR) and priority intelligence requirements (PIR).

Consequence Management—For the purpose of this Instruction, consequence management is those measures taken to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses and individuals affected by the consequences of a CBRNE situation. For domestic consequence management, the primary authority rests with the States to respond. The Federal Emergency Management Agency (FEMA) is the Lead Federal Agency (LFA) for domestic consequence management and the Department of State (DoS) is the LFA for foreign consequence management.

Coordination—The necessary action to ensure adequate exchange of information to integrate, synchronize and deconflict operations between separate organizations. Coordination is not necessarily a process of gaining approval, but is most often used for mutual exchange of information. Normally used between functions of a supporting staff. Direct liaison authorized (DIRLAUTH) is used to coordinate with an organization outside of the immediate staff or organization.

Counterintelligence (CI)—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 persons, or international terrorist activities.

Criminal Intelligence (CRIMINT)—Law enforcement information derived from the analysis of information collected through investigations, forensics, crime scene and evidentiary processes to establish intent, history, capability, vulnerability and modus operandi of threat and criminal elements.

Crisis Management—For the purpose of this Instruction, crisis management is those measures taken to resolve a hostile situation and to investigate and prepare a criminal case for prosecution under Federal law. Crisis management shall include a response to an incident involving WMD, an improvised explosive device, or a hostage crisis that is beyond the capability of the LFA.

Critical Asset—An asset that is of such extraordinary importance that its incapacitation or destruction would have a serious, debilitating effect on the ability of one or more DoD Components or Defense Infrastructure Sector Lead Agents to execute the task or mission essential tasks it supports. Task Critical Assets are used to identify defense critical assets.

Criticality Assessment—For the purposes of this Instruction, an assessment of the effect of temporary or permanent loss of key assets or infrastructures on the installation or a unit's ability to perform its mission. The assessment also examines costs of recovery and reconstitution including time, funds, capability and infrastructure support.

Defense Critical Asset—An asset of such extraordinary importance to DoD operations in peace, crisis and war that its incapacitation or destruction would have a very serious, debilitating effect on the ability of the Department of Defense to fulfill its mission.

Defense Critical Infrastructure (DCI)—Department of Defense and non-Department of Defense networked infrastructure essential to project, support and sustain military forces and operations worldwide.

Design Basis Threat (DBT)—The threat upon which a system of countermeasures protecting assets is based. The design basis threat includes the aggressor tactics and the associated weapons, explosives, tools, and agents.

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.

DoD AT Program—The minimum elements of the DoD AT program as a whole and of DoD Component AT programs are AT risk management, planning, training and exercises, resource application and program review.

DoD Civilian Work Force—U.S. citizens or foreign nationals working for the Department of Defense and paid from appropriated or non-appropriated funds under permanent or temporary appointment. This includes employees filling full-time, part-time, intermittent or on-call positions. Specifically excluded are all government contractor employees.

DoD Component—The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the combatant commands, the Office of the Inspector General of the Department of Defense, the Department of Defense Agencies, field activities and all other organizational entities in the Department of Defense.

DoD Contractor—Any individual, firm, corporation, partnership, association or other legal non-Federal entity that enters into a contract directly with the Department of Defense to furnish services, supplies or both, including construction. Defense contractors may include U.S. nationals, local citizens or third country nationals. Defense contractors do not include foreign governments or representatives of foreign governments that are engaged in selling to the Department of Defense or a DoD Component or foreign corporations wholly owned by foreign governments.

DoD Elements and Personnel—For the purposes of this Instruction, DoD military and civilian personnel and their dependent family members; DoD contractors; DoD installations and facilities; DoD-owned, leased or managed defense critical infrastructure.

DoD Personnel—For the purposes of this Instruction, Uniformed Military Service members and DoD Federal civilian employees hired and paid from appropriated and non-appropriated funds under permanent or temporary appointment.

Eagle Eyes Program—A CSAF-approved Air Force antiterrorism defensive program created to enhance the collection of threat information by educating members of the Total Force and off-base citizens on the nature of terrorist attack-planning activities. The program also establishes 24-hour phone numbers to call when suspicious behavior is observed.

Emergency Responders—The response elements of a Disaster Response Force (DRF) that deploy to the accident scene after the First Responders to expand Command and Control and perform support functions. Emergency Responders include follow-on elements such as firefighters, law enforcement personnel, security personnel, and emergency medical technicians, as well as emergency management personnel, EOD personnel, physicians, nurses, medical treatment providers at medical treatment facilities, public health officers, bioenvironmental engineering personnel, and mortuary affairs personnel. Emergency Responders also include specialized teams such as the Emergency Management Support Team (EMST) or Shelter Management Team (SMT). Not all Emergency Responders are First Responders, but all First Responders are Emergency Responders. First Responders are not assigned as augmentees or to additional duties that will conflict with their emergency duties. For further information on DRF, EMST and SMT see AFI 10-2501.

Facility—A real property entity consisting of one or more of the following: a building, a structure, a utility system, pavement and underlying land.

Family Member—Individuals defined as Dependents in Section 1072(2) of Title 10 U.S.C.

First Responder—The DRF elements that deploy immediately to the disaster scene to provide initial C2, to save lives, and to suppress and control hazards. Firefighters, law enforcement/security personnel, key medical personnel, and EOD during IED and nuclear accident response operations provide the initial, immediate response to a CBRNE incident. All First Responders are Emergency Responders, but not all Emergency Responders are First Responders.

Food and Water Security—The protection of food and water sources from disruption and contamination or other terrorist acts that could severely impact operations. Food and water security measures include those actions taken to detect, prevent and mitigate the effects from intentional acts designed to disrupt or contaminate food and water sources.

Force Health Protection (FHP)—A comprehensive threat-based program directed at preventing and managing health-related actions against Air Force uncommitted combat power.

Force Protection (FP)—Actions taken to prevent or mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities and critical information. These actions conserve the force's fighting potential so it can be applied at the decisive time and place and incorporate the coordinated and synchronized offensive and defensive measures to enable the effective employment of the joint force while degrading opportunities for the enemy. Force protection does not include actions to defeat the enemy or protect against accidents, weather or disease (JP 1-02). [The process of detecting threats and hazards to the Air Force and its mission, and applying measures to deter, preempt, negate, or mitigate them based on an acceptable level of risk (AFDD 3-10). The Air Force's integrated approach demands that actions to both defeat the enemy and protect against hazards such as accidents, weather, disease, and natural disasters be incorporated in how the AF defines Force Protection.]

Force Protection Condition (FPCON)—A DoD-approved system standardizing the Department's identification, recommended preventive actions and responses to terrorist threats against U.S. personnel and facilities. This system is the principal means for a commander to apply an operational decision on how to protect against terrorism. It facilitates inter-Service coordination and support for AT activities.

Force Protection Detachment (FPD)—A CI element that provides comprehensive CI support to transiting ships, personnel and/or aircraft in regions of elevated threat.

Force Protection Intelligence (FPI)—Analyzed, all-source intelligence that, when integrated or fused with other FP information, provides an assessment of the threats to DoD mission, people or resources. FPI is proactive and drives FP decisions in support of the commander's intent.

High-Risk Billet (HRB)—Authorized personnel billet (designated by the appropriate authority as identified in DoDI O-2000.22) that because of grade (normally, General, Admiral or Senior Executive Service equivalent), assignment (assigned in a country with a DIA terrorist threat level of Significant or higher), travel itinerary or symbolic value may make a person filling it an especially attractive or accessible terrorist target.

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

Higher Headquarters Assessment (HHA)—An overall assessment by a higher headquarters of how an organization is managing its AT program, including management and compliance efforts by subordinate organizations.

Installation—A grouping of facilities, located in the same vicinity, which support particular functions. Installations may be elements of a base.

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

Integrated Defense—Integrated Defense is the application of active and passive defense measures, employed across the legally-defined ground dimension of the operational environment, to mitigate potential risks and defeat adversary threats to Air Force operations. Also called ID (AFPD 31-1).

Intelligence—1.) The product resulting from the collection, processing, integration, evaluation, analysis and interpretation of available information concerning foreign countries or areas. 2). The information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. [The term is also applied to the activity which results in the product and to the organizations engaged in such activity.]

Joint Staff Integrated Vulnerability Assessment (JSIVA)—A vulnerability-based evaluation of an installation's ability to deter and/or respond to a terrorist incident. A vulnerability-based assessment considers both the current threat and the capabilities that may be employed by both transnational and local terrorist organizations, both in terms of their mobility and the types of weapons historically employed.

Mutual Aid Agreement (MAA)—A written agreement between agencies or jurisdictions in which they agree to assist each other on request by furnishing personnel and equipment.

Physical Security—For the purposes of this Instruction, 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.

Priority Intelligence Requirement (PIR)—Those intelligence requirements for which a commander has an anticipated and stated priority in the task of planning and decision-making.

Program Review—A review conducted to evaluate the effectiveness and adequacy of AT program implementation. The evaluation shall include an assessment of the degree to which AF AT Programs comply with the standards prescribed in this instruction.

Protection Providing Organization (PPO)—Refers collectively to the U.S. Army Criminal Investigation Command, the Naval Criminal Investigative Service, Air Force Office of Special Investigations, the Defense Criminal Investigative Service, the Pentagon Force Protection Agency, and the National Security Agency.

Protective Services—A specialized activity, which increases the personal safety and security of a distinguished visitor or other principal. The activity may be limited to a protective threat assessment or may extend to a major PSD involving considerable manpower and resources.

Protective Service Detail (PSD)—Trained and armed protective security officials capable of providing continuous protection for a designated individual.

Security—For the purposes of this Instruction, measures taken by a military unit, activity, or installation to protect against all acts designed to, or that may, impair its effectiveness. Also, a condition that results from establishing and maintaining protective measures that ensures a state of inviolability from hostile acts or influences.

Separate Facility—A real property entity consisting of one or more of the following: a building, a structure, a utility system, pavement and underlying land that is separate from an installation and has inherent responsibility for emergency response functions, e.g., 911 response functions.

Special Event—An activity characterized by a large concentration of personnel and/or a gathering where distinguished visitors are involved, often associated with a unique or symbolic event.

Support Agreement—Written agreement between agencies, organizations, or jurisdictions that they will assist one another on request by furnishing personnel, equipment, or expertise in a specified manner. Reciprocal assistance between a local government and an installation for emergency services under a pre-arranged plan. Mutual aid is synonymous with mutual assistance, outside aid, memorandums of understanding, memorandums of agreement, letters of agreement, cooperative assistant agreement, intergovernmental compacts, or other similar agreements, written or verbal, that constitute an agreed reciprocal assistance plan for sharing emergency services. MAAs between entities are an effective means to obtain resources and should be developed whenever possible. MAAs should be in writing, be reviewed by legal counsel, and be signed by a responsible official.

TACON for FP—TACON that enables the GCC to order implementation of FP measures and to exercise the security responsibilities outlined in any MOA concluded pursuant to MOU between DOS and DoD, and Security of DoD Elements and Personnel in Foreign Areas (known as the Universal MOU). Further, TACON for FP authorizes the GCC to change, modify, prescribe and enforce FP measures for covered forces. This relationship includes the authority to inspect and assess security requirements, and direct DoD activities to identify the resources required to correct deficiencies and submit budget requests to parent organizations to fund identified corrections. The GCC may also direct immediate FP measures (including temporary relocation and departure) when in his or her judgment such measures must be accomplished without delay to ensure the safety of the DoD personnel involved. Persons subject to TACON for FP of a GCC include Active and Reserve Component personnel (including National Guard personnel in a Title 10 status (Sections 134 and 1072(2)) in the AOR as well as all DoD civilian employees and their family members in the AOR.

Terrorism—The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

Terrorism Consequence Management—DoD preparedness and response for mitigating the consequences of a terrorist incident, including the terrorist use of WMD. DoD consequence management activities are designed to support the lead Federal agency (domestically, the Department of Homeland Security; foreign, the Department of State) 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 Incident Response Measures—A set of procedures established for response forces to deal with the effects of a terrorist incident.

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

Terrorism Threat Level (TTL)—An intelligence threat assessment of the level of terrorist threat faced by U.S. personnel and interests. The assessment is based on a continuous intelligence analysis of a minimum of four elements: terrorist group operational capability, intentions, activity and operational environment. There are four threat levels: LOW, MODERATE, SIGNIFICANT and HIGH. Threat levels should not be confused with FPCONs. Threat-level assessments are provided to senior leaders to assist them in determining the appropriate local FPCON.

Terrorist—An individual who commits an act or acts of violence or threatens violence in pursuit of political, religious, or ideological objectives.

Terrorist Groups—Any number of terrorists who assemble together, have a unifying relationship, or are organized for the purpose of committing an act or acts of violence or threatens violence in pursuit of their political, religious, or ideological objectives.

Unit—1. Any military element whose structure is prescribed by competent authority, such as a table of organization and equipment; specifically, part of an organization. 2. An organization title of a subdivision of a group in a task force. 3. With regard to Reserve Components of the Armed Forces, denotes a Selected Reserve unit organized, equipped and trained for mobilization to serve on active duty as a unit or to augment or be augmented by another unit.

Unit Antiterrorism Representative—The principal military or civilian advisor charged with managing the AT program for a unit or DoD element not required to have an ATO as stipulated in Standard 9.

Vulnerability—In AT, a situation or circumstance which, if left unchanged, may result in the loss of life or damage to mission-essential resources. It includes the characteristics of an installation, system, asset, application, or its dependencies that could cause it to suffer a degradation or loss (incapacity to perform its designated function) as a result of having been subjected to a certain level of threat or hazard.

Vulnerability Assessment (VA)—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)—Chemical, biological, radiological, or nuclear weapons capable of a high order of destruction or causing mass casualties; excludes the means of transporting or propelling the weapon where such means is a separable and divisible part from the weapon.

Attachment 1 (30SW)

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

30SWVA 10-1, *Force Protection Condition (FPCON) Alpha (Green Background), 1 August 2011*

30SWVA 10-1A, Force Protection Condition (FPCON) Alpha "Exercise" (Green Background), 1 August 2011

30SWVA 10-2, *Force Protection Condition (FPCON) Bravo (Yellow Background), 1 August 2011*

30SWVA 10-2A, *Force Protection Condition (FPCON) Bravo "Exercise" (Yellow Background), 1 August 2011*

30SWVA 10-3, *Force Protection Condition (FPCON) Charlie (Orange Background), 1 August 2011*

30SWVA 10-3A, *Force Protection Condition (FPCON) Charlie "Exercise" (Orange Background), 1 August 2011*

30SWVA 10-4, *Force Protection Condition (FPCON) Delta (Red Background), 1 August 2011*

30SWVA 10-4A, *Force Protection Condition (FPCON) Delta "Exercise" (Red Background), 1 August 2011*

30SWVA 10-5, *Force Protection Condition (FPCON) Normal (White Background), 1 August 2011*

30SWVA 10-6, *Threat Awareness Memory Jogger, 1 August, 2011*

30SWVA 10-7, *Suspicious Package/Letter/Unattended Item, 1 August, 2011*

30SWVA 10-8, S*uspicious Powders or Substances, 1 August, 2011*

30SWVA 10-9, *Bomb Threats, 1 August, 2011*

Acronyms and Abbreviations

VA – Visual Aid

30 SW – 30th Space Wing

VAFB – Vandenberg Air Force Base

Attachment 2

FORCE PROTECTION CONDITION (FPCON) MEASURES

A2.1. General. The DoD FPCON System describes the progressive level of protective measures that are implemented by all the DoD Components in anticipation of or in response to a terrorist threat or attack. The FPCON System is the principal means through which commanders apply an operational decision on how to best guard against the terrorist threat. The protective measures identified in the FPCON System assist commanders in reducing the risks of terrorist attacks and other security threats to DoD personnel, units and activities. The measures below are derived from DoD AT Standard 22 (DODI 2000.16, Enclosure 4, *DoD FPCON*) and include AF modifications. Commanders will ensure these measures and developed measures address local and operational risks. Commanders must consider GCC policies, local laws, mutual support agreements and/or the SOFA. Air Force commanders are responsible for implementing FPCON measures.

A2.1.1. Commanders shall ensure the following when implementing FPCON measures:

A2.1.1.1. Ensure there is an effective AT plan and the plan is widely known and practiced in order to use every airman as a sensor.

A2.1.1.2. Analyze the threat and plan courses of action to defeat those threats. Detailed planning against plausible enemy courses of action will often point to vulnerabilities which can be mitigated through adjustments to TTPs and further mitigated through innovation and programming.

A2.1.1.3. Consider force-on-force, “red team,” or intruder exercises to test COAs. Development and implementation of effective friendly COAs to counter known threats offers a reasonable deterrent effect and the opportunity for long-term success against terrorist attack.

A2.1.1.4. Ensure personnel assigned tasks directed by FPCON measures are properly trained and available to carry out the tasks.

A2.1.1.5. Based on the threat, employ sufficient patrols to deter enemy action, disrupt terrorist planning and respond to incidents or attacks against the installation. Patrols should focus protection on critical operational assets, mission support infrastructure and mass gathering locations.

A2.1.1.6. Consider placing barriers to create standoff around identified critical assets, facilities with BSAT, restricted areas, high-occupancy facilities, flight line entry points and high value resource areas.

A2.1.1.7. Review and be familiar with mutual aid and host-tenant support agreements. Keep law enforcement agencies (federal, state and local) appraised of the current situation and threat to determine the level of incident support the installation provides or receives.

A2.1.1.8. Ensure the installation Disaster Response Force and its sub elements are trained and available for response as described in AFI 10-2501.

A2.1.2. The DoD FPCON System consists of five progressive levels of increasing AT protective measures.

A2.1.3. Site-specific AT measures and physical security actions, linked to a FPCON, shall be classified CONFIDENTIAL. When separated from the AT plan, specific AT measures linked to a FPCON and site-specific FPCON levels may be downgraded to FOR OFFICIAL USE ONLY, if appropriate.

A2.1.4. Upon declaration of a FPCON level, all listed security measures for that FPCON level shall be implemented immediately unless waived in writing by the appropriate GCC or delegated representative. In non-DoD controlled facilities housing DoD occupants, DoD organizations shall implement applicable FPCON measures in space directly controlled by DoD to the extent possible. The supplementing RAMs and command-unique or site-specific measures should also be implemented to complicate a terrorist group's operational planning and targeting.

A2.1.5. AF installations and separate facilities shall supplement each FPCON measure in this instruction with site-specific details describing how the measure is to be implemented locally, to include responsibilities assigned to subordinate units and organizations.

A2.1.6. Air field-specific measures are for installations and facilities with a permanently functioning air field. Installations and facilities with an emergency helicopter pad should review and implement any applicable air field-specific measures when they anticipate air operations.

A2.1.7. The CBRNE-related FPCON measures contained in this publication are not all inclusive. Additional CBRNE FPCON measures are in the AF Civil Engineer Support Agency (AFCESA) CEMP 10-2 template and AFMAN 10-2503, *Operations in a Chemical, Biological, Radiological, Nuclear, and High- Yield Explosive (CBRNE) Environment*. Each MAJCOM and installation should also develop additional CBRNE FPCON measures applicable to their location.

A2.2. FPCON NORMAL. This condition applies when a general global threat of possible terrorist activity exists and warrants a routine security posture. At a minimum, access control will be conducted at all DoD installations and facilities.

A2.2.1. Measure NORMAL 1: Secure and randomly inspect buildings, rooms and storage areas not in regular use.

A2.2.2. Measure NORMAL 2 (AF Modified): Conduct random security checks of vehicles and persons entering facilities under the jurisdiction of the United States.

A2.2.2.1. Measure NORMAL 2.1 (AF Added): Conduct random vehicle inspections at installation entry points in addition to Random Installation Entry/Exit Vehicle Check (RIEVC) as directed by installation commanders. Implement 100% inspection of large commercial vehicles. MAJCOM and local planners should define large commercial vehicles in IDPs based on geographical location, character of local transport and threat. Conduct random vehicle inspections at entrances to restricted areas beyond inspection requirements listed in AFI 31-101.

A2.2.3. Measure NORMAL 3: Limit access points for vehicles and personnel commensurate with a reasonable flow of traffic.

A2.2.4. Measure NORMAL 4 (AF Modified): Identify defense critical infrastructure and critical assets, facilities with BSAT, and high-occupancy buildings.

A2.2.5. Measure NORMAL 5 (AF Added): Implement a daily RAM program involving the entire installation with emphasis on identifying surveillance activities and disrupting the terrorist attack cycle. Installations will tailor their RAM program to meet the threat and mitigate vulnerabilities.

A2.2.6. Measure NORMAL 6 (AF Added): Conduct 100% "hands on" identification verification of all vehicle operators and pedestrians entering installations. When available, employ the Defense Biometric Identification System (DBIDS) to validate identification credentials.

A2.2.7. Measure NORMAL 7 (AF Added): Where no permanent channeling measures are built into the gates, emplace barriers or obstacles on in-bound and out-bound lanes at installation entry points to mitigate high-speed installation access through entry and exit lanes, IAW UFC 4-022-01. Prevent base entry through exit lanes. Ensure sufficient number and types of barriers remain for increased FPCON/RAMs.

A2.2.8. Measure NORMAL 8 (AF Added): Identify local vendors that are able to provide rapid stocks of emergency response equipment and supplies IAW local response plans.

A2.3. FPCON ALPHA (AF Modified). 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 FPCON must be capable of being maintained indefinitely.

A2.3.1. Measure ALPHA 1: Fully implement all measures of FPCON NORMAL.

A2.3.2. Measure ALPHA 2: At regular intervals, inform personnel and family members of the general situation. Ensure personnel arriving for duty are briefed on the threat. Also, remind them to be alert for and to report suspicious activities, such as the presence of unfamiliar personnel and vehicles, suspicious parcels and possible surveillance attempts.

A2.3.2.1. Measure ALPHA 2.1 (AF Added): Post signs at installation gates and utilize mass communication systems to inform/remind personnel of the FPCON level.

A2.3.3. Measure ALPHA 3: The duty officer or personnel with access to building plans as well as the plans for area evacuations must be available at all times. Plans should be in place to execute access control procedures. Key personnel required to implement security plans should be on-call and readily available.

A2.3.4. Measure ALPHA 4 (AF Modified): Increase random security checks of vehicles and persons entering installations or facilities under the jurisdiction of the United States.

A2.3.5. Measure ALPHA 5: Initiate food and water risk management procedures, brief personnel on food and water security procedures and report any unusual activities.

A2.3.6. Measure ALPHA 6 (AF Modified): Test mass notification systems weekly.

A2.3.7. Measure ALPHA 7: Review all plans, identify resource requirements and be prepared to implement measures of the next higher FPCON level.

A2.3.7.1. Measure ALPHA 7.1 (AF added): Review and be prepared to implement plans (to include AT, CEMP 10-2, IDP, MCRP/Mass Casualty Plan, Disease Containment Plan (DCP), etc.) and most recent VA reports, and identify resource requirements. Review dependent, civilian and military personnel evacuation plans and support agreements with local officials.

A2.3.8. Measure ALPHA 8 (AF Modified): Review and, if necessary, implement security measures for DoD identified HRP IAW DoDI O-2000.22 and AFI 71-101, Volume 2.

A2.3.9. Measure ALPHA 9 (AF Modified): Consult local authorities on the threat and mutual AT measures. As appropriate, brief law enforcement agencies who provide support to the installation and request assistance as necessary to ensure protection of resources and personnel.

A2.3.10. Measure ALPHA 10: Review intelligence, CI and operations dissemination procedures.

A2.3.11. Measure ALPHA 11: Review barrier plans.

A2.3.12. Measure ALPHA 12 (AF Added): Secure access to all bulk quantity storage areas containing hazardous and flammable material.

A2.3.13. Measure ALPHA 13 (AF Added): Review and be prepared to implement CBRNE detection plan, ensuring it uses available detectors (deployment and home station assets).

A2.3.14. Measure ALPHA 14: Review all higher FPCON measures.

A2.3.15. Measure ALPHA 15 (AF Added): Review and be prepared to implement plans for centralized mail handling.

A2.4. FPCON BRAVO. Applies when an increased or more predictable threat of terrorist activity exists. Sustaining BRAVO measures for a prolonged period may affect operational capability and military-civil relationships with local authorities.

A2.4.1. Measure BRAVO 1: Fully implement all measures of lower FPCON levels.

A2.4.1.1. Measure BRAVO 1.1 (AF Added): Brief personnel on the updated threat and associated procedures. Update signs at installation gates and utilize mass communication systems to inform/remind personnel of the FPCON level.

A2.4.1.2. Measure BRAVO 1.2 (AF Added): Increase frequency of daily RAMs. Focus additional RAMs on current situation and nature of threat.

A2.4.1.3. Measure BRAVO 1.3 (AF Added): Have intelligence and OSI provide a CBRNE threat briefing to the Threat Working Group (TWG) or equivalent, if there is a threat of CBRNE. Include specific information such as probability of CBRNE use, type(s) and amount of CBRNE material, likely CBRNE material release mechanisms and probable targets.

A2.4.1.4. Measure BRAVO 1.4 (AF Added): Verify the interoperability of CBRNE response procedures with local community resources, to include activities outlined in the CEMP 10-2, DCP, and MCRP.

A2.4.1.5. Measure BRAVO 1.5 (AF Added): Contact local hospitals and establish/ensure lines of communication for notification of the installation in the event of

significant increase in antibiotic use or people exhibiting symptoms of exposure to CBRNE materials.

A2.4.2. Measure BRAVO 2 (AF Modified): Enforce control of entry into facilities containing defense critical infrastructure and critical assets, BSAT, lucrative targets, or high-profile locations. Randomly search vehicles entering these areas. Particular scrutiny should be given to vehicles that are capable of concealing a large explosive device sufficient to cause catastrophic damage to property or loss of life (e.g., cargo vans or delivery vehicles).

A2.4.3. Measure BRAVO 3 (AF Modified): Keep cars and objects (e.g., crates, trash containers) away from buildings to reduce vulnerability to bomb attacks. Apply this criterion to all critical and high-occupancy buildings (consider applying to all inhabited structures to the greatest extent possible). Standoff distance should be determined by the following factors: asset criticality, the protection level provided by the structure, and IED or Vehicle Borne IED (VBIED) threat and available security measures. Consider centralized parking and implementation of barrier plans. Utilize UFC 4-010-01 and UFC 4-010-02. AFH 10-2401, *Vehicle Bomb Mitigation Guide (FOUO)*, is an additional tool for standoff planning.

A2.4.4. Measure BRAVO 4: Secure and periodically inspect all buildings, rooms and storage areas not in regular use.

A2.4.5. Measure BRAVO 5: At the beginning and end of each workday, as well as at random intervals, inspect the interior and exterior of buildings in regular use for suspicious packages.

A2.4.6. Measure BRAVO 6: Implement mail-screening procedures to identify suspicious letters and parcels.

A2.4.7. Measure BRAVO 7: Randomly inspect commercial deliveries. Advise family members to check home deliveries.

A2.4.7.1. Measure BRAVO 7.1 (AF Added): Increase random security checks of vehicles and persons entering installations or facilities under the jurisdiction of the United States. Inspect all commercial deliveries (AF Baseline FPCON posture directs inspection of all large commercial vehicles in FPCON NORMAL).

A2.4.8. Measure BRAVO 8 (AF Modified): Randomly inspect food and water for evidence of tampering or contamination before use by DoD personnel. Inspections should include delivery vehicles, storage areas/facilities and storage containers.

A2.4.9. Measure BRAVO 9: Increase security measures and guard presence or initiate increased patrols and surveillance of DoD housing areas, schools, messes, on-base clubs, military treatment facilities and similar high-occupancy targets to improve deterrence and defense, and to build confidence among staff and family members.

A2.4.10. Measure BRAVO 10: Implement plans to enhance off-installation security for DoD facilities. In areas with Threat Levels of Moderate, Significant, or High, coverage includes facilities (e.g., DoD schools and daycare centers) and transportation services and routes (e.g., bus routes) used by DoD employees and family members.

A2.4.11. Measure BRAVO 11: Inform local security committees of actions being taken.

A2.4.11.1. Measure BRAVO 11.1 (AF Added): Consult local authorities on the threat and mutual AT measures. As appropriate, brief law enforcement agencies who provide support to the installation and request assistance as necessary to ensure protection of resources and personnel. As appropriate, coordinate with local authorities regarding infrastructure outside the installation, e.g., infrastructure supplying energy to the installation. NOTE: The following Transportation Protection Procedures are implemented during this measure. Postpone non-essential movements of Arms Ammunition and Explosives (AA&E) Category I and II items, classified munitions, and ship by military air if feasible. Plan for possible use of the installation as a DoD Safe Haven and review physical security standards in AA&E holding areas. Consider liaison with civil authorities to review specific local threat conditions or convene the Threat Working Group (TWG) to address the threat situation and possible additional protective measures.

A2.4.12. Measure BRAVO 12 (AF Modified): Verify identity of visitors to the installation and randomly inspect their suitcases, parcels and other containers. Visitors are non-DoD affiliated personnel who do not have official DoD credentials authorizing installation access.

A2.4.13. Measure BRAVO 13: Conduct random patrols to check vehicles, people and buildings.

A2.4.14. Measure BRAVO 14: As necessary, implement additional security measures for High-Risk Personnel (HRP).

A2.4.15. Measure BRAVO 15: Place personnel required for implementing AT plans on call; commanders should exercise discretion in approving absences.

A2.4.16. Measure BRAVO 16: Identify and brief personnel who may augment guard forces. Review specific rules of engagement including the use of deadly force.

A2.4.17. Measure BRAVO 17: As deemed appropriate, verify identity of personnel entering buildings.

A2.4.18. Measure BRAVO 18: Review status and adjust as appropriate operations security, communications security and information security procedures.

A2.4.19. Measure BRAVO 19 (AF Modified): (Airfield-specific) Limit access points in order to enforce entry control. As appropriate, erect barriers and establish manned checkpoints at entrances to airfields. Verify the identity of all individuals entering the airfield (flight line and support facilities) with no exceptions. Randomly inspect vehicles, briefcases and packages entering the airfield.

A2.4.20. Measure BRAVO 20: (Airfield-specific) Coordinate plans to safeguard aircraft departure and approach flight paths with local authorities. Be prepared to activate contingency plans and issue detailed air traffic control procedures. As appropriate, take actions to mitigate the threat of surface- to-air missiles or standoff weapons that can be delivered from beyond the airfield perimeter.

A2.4.21. Measure BRAVO 21 (AF Added): Ensure CBRNE detectors are operational as outlined with the detection plan (deployment and home station assets).

A2.4.22. Measure BRAVO 22: Review all higher FPCON measures.

A2.5. FPCON CHARLIE. Applies when an incident occurs or intelligence is received indicating that some form of terrorist action or targeting against personnel or facilities is likely. Prolonged implementation of CHARLIE measures may create hardship and affect the activities of the unit and its personnel.

A2.5.1. Measure CHARLIE 1: Fully implement all measures of lower FPCON levels.

A2.5.1.1. Measure CHARLIE 1.1 (AF Added): Conduct 100% identification checks of all personnel entering the installation, to include vehicle passengers.

A2.5.1.2. Measure CHARLIE 1.2 (AF Added): Brief personnel on the updated threat and associated procedures. Update signs at installation gates and utilize mass communication systems to inform/remind personnel of the FPCON level. If a CBRNE threat exists, ensure the Disaster Response Force and, if permissible, local authorities are briefed on the threat.

A2.5.1.3. Measure CHARLIE 1.3 (AF Added): Increase frequency of daily RAMs. Focus additional RAMs on current situation and nature of threat.

A2.5.2. Measure CHARLIE 2: Recall additional required personnel. Ensure armed augmentation security personnel are aware of current rules of engagement and any applicable Status of Forces Agreements (SOFA). Review types of weapons and ammunition issued to augmentation security personnel; heightened threats may require employment of different weapon capabilities.

A2.5.3. Measure CHARLIE 3: Be prepared to react to requests for assistance from both local authorities and other installations in the region.

A2.5.3.1. Measure CHARLIE 3.1 (AF Added): Ensure flow of information between on and off-base medical treatment facilities participating in the medical surveillance program. Consider initiation of manual collection of data if the automated system has a 24-hour or more delay in providing results.

A2.5.3.2. Measure CHARLIE 3.2 (AF Added): Consider Noncombatant Evacuation Operations (NEO).

A2.5.4. Measure CHARLIE 4: Limit access points in order to enforce entry control. Randomly search vehicles.

A2.5.4.1. Measure CHARLIE 4.1 (AF Added): Increase random security checks of vehicles and persons entering installations or facilities under the jurisdiction of the United States.

A2.5.4.2. Measure CHARLIE 4.2 (AF Added): Implement procedures to expedite the entry of first and emergency responders onto the installation during emergencies. Ensure these procedures prevent unauthorized entry.

A2.5.5. Measure CHARLIE 5: Ensure or verify the identity of all individuals entering food and water storage and distribution centers using sign-in and sign-out logs at access control and entry points, and limit or inspect all personal items.

A2.5.6. Measure CHARLIE 6 (AF Modified): Initiate contingency (credible CBRNE threat) monitoring for chemical, biological and radiological contamination as required. Suspend contractors and off-facility users from tapping into the facility water system. An alternate

locally-developed measure should be implemented when contractors are responsible for DoD water supplies or when water is provided by local (non-DoD) sources or agencies.

A2.5.6.1. Measure CHARLIE 6.1 (AF Added): If a CBRNE threat exists, ensure all shortages of C-CBRNE equipment and its potential impact is briefed to the installation commander.

A2.5.6.2. Measure CHARLIE 6.2 (AF Added): Verify operation, deploy and begin using all available CBRNE detectors (deployment and home station) as outlined in the detection plan.

A2.5.7. Measure CHARLIE 7: Increase standoff from sensitive buildings based on the threat. Implement barrier plan to hinder vehicle-borne attack.

A2.5.8. Measure CHARLIE 8 (AF Modified): Increase patrolling of the installation/facility to include waterside perimeters, if appropriate. Be prepared to assist local authorities in searching for threats outside the facility perimeter. For airfields, patrol or provide observation of aircraft parking areas and approach and departure flight corridors as appropriate to the threat (coordinate with Transportation Security Administration, Marine Patrol, United States Coast Guard and local law enforcement as required to cover off-facility approach and departure flight corridors).

A2.5.9. Measure CHARLIE 9 (AF Modified): Increase protection for all defense critical infrastructure, critical assets or BSAT facilities. Give special attention to and coordinate with local authorities regarding infrastructure outside the military establishment.

A2.5.9.1. Measure CHARLIE 9.1 (AF Added): Consider closing or enhancing security at remote sites and alternate, practice or training airfields.

A2.5.9.2. Measure CHARLIE 9.2 (AF Added): Protect DoD personnel at vulnerable mass gathering facilities during peak usage, especially near the installation perimeter. Coordinate protection of mass gathering facilities off the installation with civilian law enforcement agencies.

A2.5.10. Measure CHARLIE 10: To reduce vulnerability to attack, consult local authorities about closing public (and military) roads and facilities and coordinate any other precautionary measures taken outside the installation perimeter. NOTE: The following Transportation Protection Procedures are implemented during this measure. Provide armed military escort in separate military vehicles for all AA&E Category I and II items and classified munitions and conduct liaison with state and/or local law enforcement officials prior to off-base movements.

A2.5.11. Measure CHARLIE 11: Randomly inspect suitcases, briefcases and packages being brought onto the installation through access control points and consider randomly searching them upon leaving the installation.

A2.5.12. Measure CHARLIE 12: Review personnel policy procedures to determine appropriate courses of action for dependent family members.

A2.5.13. Measure CHARLIE 13: Review access procedures for all non-U.S. personnel and adjust as appropriate. For airfields, consider terminating visitor access to the flight line and support facilities.

A2.5.14. Measure CHARLIE 14: Consider escorting children to and from DoD schools (among options to consider are escorting school buses, recommending parents escort children to/from school, etc.). Review school closure procedures with the local school district.

A2.5.15. Measure CHARLIE 15: (Airfield-specific) Reduce flying to only essential operational flights. Implement appropriate flying countermeasures as directed by the Flight Wing Commander (military aircraft) or Transportation Security Administration (civilian aircraft). Consider relief landing ground actions to take for aircraft diversions into and out of an attacked airfield. Consider augmenting fire-fighting details.

A2.5.15.1. Measure CHARLIE 15.1 (AF Added): Consider aircraft dispersal, or the dispersal of other high value assets, based on assessment of local threat from standoff weapons, vulnerability of the assets and operational feasibility.

A2.5.16. Measure CHARLIE 16: Review all FPCON DELTA measures.

A2.6. 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. FPCON DELTA is usually declared as a localized condition. FPCON DELTA measures are not intended to be sustained for an extended duration.

A2.6.1. Measure DELTA 1 (AF Modified): Fully implement all measures of lower FPCON levels. As necessary, brief personnel on the updated threat and associated procedures and update signs at installation gates, utilize mass communication systems to inform/remind personnel of the FPCON level.

A2.6.2. Measure DELTA 2: Augment guards as necessary.

A2.6.3. Measure DELTA 3: Identify all vehicles within operational or mission support areas.

A2.6.4. Measure DELTA 4: Search all vehicles and their contents before allowing entrance to the installation. Selected pre-screened and constantly secured vehicles used to transport escorted very important personnel may be exempted.

A2.6.5. Measure DELTA 5: Control facility access and implement positive identification of all personnel with no exceptions.

A2.6.6. Measure DELTA 6: Search all personally carried items (e.g., suitcases, briefcases, packages, backpacks) brought into the installation or facility.

A2.6.7. Measure DELTA 7: Close all schools located on the installation.

A2.6.8. Measure DELTA 8: Make frequent checks of the exterior of buildings and of parking areas.

A2.6.9. Measure DELTA 9: Restrict all non-essential movement. NOTE: The following Transportation Protection Procedures are implemented during this measure. Temporarily suspend all AA&E shipments in and out of the local area except those needed for critical operational requirements; ship critical items by military air if feasible; and provide armed military escort for all AA&E shipments.

A2.6.10. Measure DELTA 10: (Airfield specific) Cease all flying except for specifically authorized operational sorties. Be prepared to deploy light aircraft and/or helicopters for

surveillance tasks or to move internal security forces. Implement, if necessary, appropriate flying countermeasures.

A2.6.11. Measure DELTA 11: (Airfield specific) As appropriate, airfields should prepare to accept aircraft diverted from other stations.

A2.6.12. Measure DELTA 12: If permitted, close public and military roads and facilities. If applicable, close military roads allowing access to the airfield.

A2.6.13. Measure DELTA 13: Begin continuous monitoring for chemical, biological and radiological contamination.

A2.6.14. Measure DELTA 14 (AF Added): If not already accomplished and a credible threat exists, initiate collective protection operations and/or Shelter In Place (SIP) operations, as explained in AFMAN 10-2503.

Attachment 3

TERRORIST THREAT LEVELS

A3.1. General. The standardized DoD methodology that describes the terrorist threat to DoD personnel, facilities and interests shall be used to determine Terrorism Threat Levels (TTL). The Defense Intelligence Agency (DIA) sets the DoD TTL for all countries. Terrorism threat levels are established as the result of all-source analysis and incorporation of GCC and Military Department input. The Joint Intelligence Task Force – Countering Terrorism coordinates country TTLs with appropriate GCCs, Services and Defense Attaches.

A3.1.1. DIA and the responsible GCC may assign different threat levels to the same country. This is possible because analysts occasionally disagree about the conclusions to be drawn from available information. Threat assessments provide information to assist commanders in determining the appropriate FPCON level and measures. FPCON level declarations remain the exclusive responsibility of commanders. Threat levels are not tied to FPCON levels in any way and should not be confused. National-level DoD organizations cannot provide all intelligence that might be needed to make FPCON level determinations. Information from regional and tactical intelligence and local law enforcement authorities must also be considered.

A3.1.2. 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.

A3.2. Terrorist Threat Levels. In assessing the terrorist threat to U.S. personnel and interests, DoD intelligence agencies use a four-step scale to describe the severity of the threat. The following lists the threat levels and the combinations of analysis-based factors used to determine the level:

A3.2.1. HIGH: Anti-US terrorists are operationally active and use large casualty producing attacks as their preferred method of operation. There is a substantial DoD presence and the operating environment favors the terrorist.

A3.2.2. SIGNIFICANT: Anti-US terrorists are present and attack personnel as their preferred method of operation or a group uses large casualty producing attacks as their preferred method, but has limited operational activity. The operating environment is neutral.

A3.2.3. MODERATE: Terrorists are present, but there are no indications of anti-US activity. The operating environment favors the host nation/US.

A3.2.4. LOW: No group is detected or the group activity is non-threatening.

A3.3. Terrorist threat levels are a product of the following four factors.

A3.3.1. 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 thousands 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 decreased threat. The ability to operate on a regional or transnational basis and the overall professionalism of the group is also assessed.

A3.3.2. Intentions. This factor is the stated desire or history of terrorist attacks against U.S. 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 U.S. interests is the other key component. Whether the group will react to high profile U.S.-led international events, such as intervention in the Balkans, is also considered and rated.

A3.3.3. 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 U.S. 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.

A3.3.4. 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 U.S. 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.

Attachment 4

RISK MANAGEMENT AND RESOURCING PROCESSES

A4.1. Overview. The commander has an inherent command responsibility to reduce risks that threaten the mission with available resources. Risk management, as described in AFPD 31-1, aids the commander in assessing risk. If the commander cannot internally correct, mitigate or assume risk, they must elevate these vulnerabilities and associated risk(s) through CVAMP. CVAMP will forward the vulnerability through the chain of command to the GCC, who will decide if the vulnerability will be reported higher.

A4.2. Resourcing. Emphasis should be placed on acquiring resources to detect, assess, warn, defend or recover in order to prevent hostile acts or mitigate the effects. It is inherent upon the organization to assess the resource requirement against other organizational unfunded or funded requirements and determine if an internal reallocation of funding is appropriate and possible. CVAMP is used to collate and track AT vulnerabilities and resourcing. The status of vulnerabilities entered into CVAMP should be documented in CVAMP.

A4.3. AF Funding Sources.

A4.3.1. Planning, Programming, Budget and Execution (PPB&E). The PPB&E process includes requests considered during the POM funding cycle. This program is for long-term planning and the funds will not be available for two to five years. Information on the PPB&E process can be found in the DoD Management Initiative Decision 913.

A4.3.2. Installation and MAJCOM budget process and commander's discretionary funds.

A4.3.3. Many PEC and/or funding appropriations (AT, Physical Security, EM, Medical, Construction, Base Defense, Base Operating Support, Communications, Weapons of Mass Destruction Threat Response, Nuclear, Biological and Chemical Defense Program, Fire Emergency Services; Sustainment Restoration and Modernization (SRM), and military construction (MILCON), etc.) may be used to fund AT resourcing activities. Commanders will consider all PEC and funding appropriation sources as authorized by law and AF policy and guidance.

A4.3.4. Use Antiterrorism Program Element 28047 as the primary funding source for manpower authorizations, antiterrorism equipment, procurement, military construction and the associated costs specifically identified and measurable to those resources and activities associated with the Air Force AT Program.

A4.3.5. Specialized funds designed for AT and the war on terrorism.

A4.4. Combatant Commander's Initiative Fund (CCIF). This program provides funds for emergency or unforeseen (emergent) high priority force protection projects or equipment. It is designed for requirements that need to be funded in the current fiscal year and provides a means for the GCC to react to unforeseen requirements from changes in a terrorist threat, threat levels, force protection doctrine/standards, as well as unanticipated requirements identified as a result of VAs, tactical operations and exercising AT plans. The fund is not intended to subsidize ongoing projects, supplement budget shortfalls, or support routine activities, which are a Service responsibility. Requests must be submitted through the responsible MAJCOM to the AF

Component Command which will submit to the appropriate GCC, and the GCC will prioritize and submit to the CJCS. Submission instructions are outlined in CJCSI 7401.1.

A4.4.1. Emergency CCIF Requirement. An unanticipated requirement created by a combination of circumstances or the resulting state that requires immediate action to prevent, deter, or respond to a terrorist act.

A4.4.2. Emergent CCIF Requirement. A newly-formed, unexpected requirement resulting from a logical consequence of unforeseen circumstances calling for prompt action.

A4.4.3. AF Component Commands to GCCs must submit requests for CCIF funds through CVAMP.

A4.4.4. Emergent requirements should be less than 2 years old. The requestor must have an approved, executable and exercised AT plan.

A4.5. Effectively Managing the Resource Allocation Process.

A4.5.1. Ensure you plan for training and maintenance costs into the out years.

A4.5.2. The ATO needs to work closely with affected functional areas, installation financial advisors/comptroller and contracting from the beginning to address requirements. This will assist in identifying the appropriation sources and funding amounts.

A4.5.3. Adequately articulating and justifying requirements is crucial.

A4.5.4. Determine all appropriate potential funding sources and submit requests through the various channels. Once a requirement is funded by a source, cancel all other requests. Note: The Joint Staff does not allow the same request to be submitted through both the PPB&E and CCIF process.

A4.5.5. There are organizations that can aid the commander in identifying technology to satisfy requirements: Physical Security Equipment Action Group (PSEAG), Technical Support Working Group (TSWG), Joint Requirement Office for Chemical, Biological, Radiological and Nuclear Defense (JRO-CBRND), and the Joint Non-Lethal Weapons Directorate (JNLWD). These organizations are separately funded to provide COTS information, rapid prototyping and research and development and/or evaluation of solutions for units in the field. They can provide information and research on technology and equipment evaluated and deemed suitable for your purpose. Additionally, they can provide field assessments to assist in identifying the optimal solutions to meet your requirements.

Attachment 5

AF APPROVED LEVEL II - ATO CERTIFICATION TRAINING COURSES

A5.1. The following courses may certify AF personnel for completion of Level II - ATO Training.

Table A5.1. Air Force Level II - ATO Training.

ACC, 99th Security Forces Group, Nellis AFB, NV. Phone: DSN 682-1603.

AFGSC, 620th Ground Combat Training Squadron, F.E. Warren AFB, WY. Phone: DSN 481-7629.

AFMC, 96th Ground Combat Training Squadron Mobile Training Team (MTT), Eglin AFB, FL. Phone: DSN 872-6172.

AFRC, 610th Security Forces Squadron Mobile Training Team (MTT), Naval AS, Fort Worth, TX. Phone: DSN 739-5101 (ext 141, 134, 127).

AFSOC, USAF Special Operations School, Hurlburt Field, FL. Phone: DSN 579-6330.

AMC, USAF Expeditionary Center, Joint Base McGuire-Dix-Lakehurst, NJ. Phone: DSN 944-4101 (ext 185).

PACAF Regional Training Center, 736th Security Forces Squadron, Andersen AB, GU. Phone: DSN 315 366-6087.

PACAF ANSER Mobile Training Team (MTT), 25 E. Street Suite M-307, Hickam AFB, HI. Phone: DSN 315 448-2481.

USAFE, Ramstein AB, GE. Phone: DSN 314 480-6006.

Attachment 6

THE ANTITERRORISM STANDARDS FOR BUILDINGS DEVIATION PROGRAM

A6.1. Deviations to Unified Facilities Criteria (UFC) 4-010-01 *Minimum AT Standards for Buildings*. At facilities where compliance with UFC minimum AT standards for buildings cannot be attained, or where deviation is appropriate, units will request deviation. Deviations should not be used to avoid costs associated with compliance, but should be used where compliance cannot be achieved.

A6.2. Overview. This program formalizes AT program risk acceptance for all facilities. The inability to meet minimum AT standards for buildings at such facilities results in a higher AT program risk that must be managed. Commanders must implement the AT deviation program where resources cannot be afforded the required protection per UFC minimum AT standards for buildings. Deviations associated with such conditions are considered permanent and require compensatory measures.

A6.2.1. Applicability. This program applies to the following types of facilities as indicated.

A6.2.1.1. New Construction. Deviations from minimum UFC AT standards for buildings are required for all new facilities that enter the planning phase after this instruction goes into effect. Subordinate commands may issue stricter guidance that requires deviations for pre-existing construction through supplementation of this instruction.

A6.2.1.2. Major Renovations. Deviations from minimum UFC AT standards for buildings are required for major renovations to existing facilities that enter the planning phase after this instruction goes into effect. Major renovations, modifications, repairs, revitalizations, and restorations are defined per UFC 4-010-01 as those whose costs exceed 50% of the plant replacement value of the existing building.

A6.2.1.3. Leased Facilities. Deviations from minimum UFC AT standards for buildings are required for all leased facilities where DoD personnel occupy leased or assigned usable office area constituting at least 25% of the usable building area. This requirement applies to new and existing leases. While the Deputy Secretary of Defense memorandum dated 12 July 2011 temporarily suspended UFC 4-010-01 requirements for lease renewals or extensions, the memorandum did not alleviate these facilities from this requirement to establish deviations. This is an interim situation until comparisons between DoD completes its assessment of DoD and interagency standards for leased space and determines which standards are appropriate.

A6.3. Categorizing Deviations. A deviation must first be categorized under either a UFC minimum AT standard for buildings or a physical security standard. If a minimum UFC AT standard for buildings is being deviated from, follow the review, approval and routing criteria outlined in this instruction. If a Physical Security Standard is being deviated from, follow the approval and routing criteria outlined in AFI 31-101, paragraph 6.8. Where the GCC with TACON for FP prescribes procedures different from those prescribed above, follow the procedures of the GCC.

A6.4. Compilation of Deviations. Consider all other deviations when requesting and approving deviations to prevent a combination of deviations from creating an overall security problem.

Individual or compilation of deviations must not cause a greater security threat or vulnerability than the problem they were originally designed to address.

A6.5. Documenting Deviations. Document deviations on AF Form 116, *Request for Deviation from Security Criteria*, and submit each deviation for formal approval. Based on the long-term nature and risk-tolerance level of these deviations, they must be incorporated into the AT Plan and assigned compensatory measures in the IDP once formal approval has been granted. Do not apply for formal approval if the directive from which you are deviating specifically states it is not necessary.

A6.5.1. Completing the AF Form 116.

A6.5.1.1. The requestor of the deviation will complete blocks 1-18. If staffed electronically, the coordination boxes in block 15 (if used) must be completed before the digital signature is affixed in block 18; once the digital signature is affixed, the coordination boxes become locked. Once the requestor signs block 18, the AF Form 116 is sent to the Reviewing Official. The Reviewing Official will complete blocks 19-24. If staffed electronically, the coordination boxes in block 21 (if used) must be completed before the digital signature is affixed in block 24; once the digital signature is affixed, the coordination boxes become locked. Once the Reviewing Official signs block 24, the AF Form 116 is sent to the Approval Authority.

A6.5.1.2. The Approval Authority will complete blocks 25-32. If staffed electronically, the coordination boxes in block 29 (if used) must be completed before the digital signature is affixed in block 32; once the digital signature is affixed, the coordination boxes become locked. Any blocks that do not apply will be marked N/A.

A6.5.1.3. Ensure that block 8 of the AF Form 116 includes the number of personnel impacted and the criticality of the facility or facility mission. In addition to the justification in block 9 of AF Form 116, provide a summary of the risk analysis performed that supports the deviation and the compensatory measures. Also within block 9 include an impact statement should the deviation be denied. Within block 10 of AF Form 116, validate that the compensatory measures are resourced for the duration of the deviation. Within block 11 of AF Form 116, state if the corrective action proposed to resolve the deviation is budgeted.

A6.5.2. Requesting Officials. Deviations from UFC minimum AT standards for buildings shall be requested by the chairperson of the installation ATEC (or equivalent).

A6.5.3. Reviewing Officials. Reviewing Officials note whether compensatory measures are considered adequate and, if not, specify additional measures. Additionally, Reviewing Officials add pertinent information in block 20 to assist the Approval Authority in validating the request if necessary. Reviewing Official for minimum UFC AT standard for buildings deviations shall be the MAJCOM A7. MAJCOM A7C and/or A7P and MAJCOM ATPM will coordinate (at minimum).

A6.5.4. Approval Authority. The Approval Authority accepts or declines the risk involved in the deviation request, approves/disapproves requests, and returns them to the requester with rationale for the decision. The Approval Authority for deviations from minimum UFC AT standards for buildings shall be the MAJCOM Vice Commander. The Approval authority for deviations from UFC AT Standards where the requester does not fall under the

MAJCOM chain of command (DRUs, FOAs, etc.) shall be the first general officer/SES in the operational chain of command.

A6.6. Reviewing, Approving, and Disapproving Deviations.

A6.6.1. MAJCOMs Responsibilities. MAJCOMs are responsible for the following:

A6.6.1.1. Address the deviation approval process in MAJCOM supplements.

A6.6.1.2. Send deviation requests involving tenant units to the tenant's MAJCOM Headquarters for coordination.

A6.6.1.3. Ensure copies of all approved deviations from minimum UFC AT standards for buildings are forwarded through the responsible AT office of the AF Component Command to the Geographic Combatant Command (GCC) with TACON FP responsibility for the installation requesting the deviation. Follow GCC guidance on the frequency and content of reporting.

A6.6.1.4. Ensure the Installation and MAJCOM ATEC (or equivalents) review all deviations annually.

A6.7. Exceptions to the Deviation Program.

A6.7.1. Pre-existing Conditions. Deviations from minimum UFC AT standards for buildings are only required for new facilities or major renovations to existing facilities that enter the planning phase after this instruction goes into effect. Major renovations, modifications, repairs, revitalizations, and restorations are defined per UFC 4-010-01 as those whose costs exceed 50% of the plant replacement value of the existing building. Note that this pre-existing condition exception DOES NOT apply to leased facilities.

A6.7.2. Directed by other security instructions. Deviations from standards established in other physical security instructions (such as AFI 31-101) shall be requested IAW procedures contained in that instruction. Use these procedures only for minimum AT standards for buildings required by UFC 4-010-01.

A6.8. Compensating for Deviations. Compensatory measures are inherently different than security measures normally in-place. Although different, they must provide a comparable level of security. Security measures, facilities, equipment, and procedures that are already required are not normally adequate as compensatory measures. Instructions consisting mainly of orders to "increase vigilance" are inadequate. Additional forces, equipment, etc., are usually necessary to ensure comparable security. However, there are some instances when existing forces may be used to compensate temporarily for deviations. All Integrated Defense (ID) contributors must be aware of deviations in their assigned areas and instruct personnel on requirements. Compensatory measures may include the following:

A6.8.1. Equipment, such as additional locks, intrusion detection systems (IDS), lighting, and barricades.

A6.8.2. Security measures that provide the same level of protection as the security standard being deviated from and compensated for as a minimum.

Attachment 7

CATEGORIES OF SUSPICIOUS ACTIVITY

A7.1. Acquisition of Expertise. Unjustified attempts to obtain or conduct specialized training in security concepts, military weapons or tactics, or other unusual capabilities such as specialized transport or handling capabilities that would cause a reasonable person to perceive a threat to DoD personnel, facilities, or forces in transit.

A7.2. Breach or Attempted Intrusion. Unauthorized entry or attempted entry into a restricted area or protected site; impersonation of authorized personnel (e.g., police, security, or janitorial personnel).

A7.3. Eliciting Information. Suspicious questioning of personnel by any means about particular DoD structures, functions, personnel, or procedures at the facility or infrastructure.

A7.4. Expressed or Implied Threat. A threat to DoD personnel or threatened damage to or compromise of a DoD facility or infrastructure.

A7.5. Flyover or Landing. Suspicious overflight of or landing near a DoD facility or infrastructure by any type of flying vehicle (e.g., airplane, helicopter, unmanned aerial vehicle, glider).

A7.6. Materials Acquisition or Storage. Acquisition of unusual quantities of precursor material (e.g., cell phones, pagers, fertilizer, fuel, and timers); unauthorized or unlicensed individual or group attempts to obtain precursor chemicals, agents, or toxic materials; or rental of storage units for the purpose of storing precursor material, chemicals, or apparatuses for mixing chemicals.

A7.7. Misrepresentation. Misusing or presenting false insignia, documents, or identification or engaging in any other activity to misrepresent one's affiliation.

A7.8. Recruiting. Building operations teams and developing contacts, or collecting personnel data, banking data, or travel data under circumstances that would cause a reasonable person to perceive a threat to DoD personnel, facilities, or forces in transit.

A7.9. Sabotage, Tampering, or Vandalism. Damaging, manipulating, or defacing part of a DoD facility, infrastructure, or protected site. Acts of vandalism committed by DoD civilian employees, military members, or their dependents should not be reported as suspicious activity unless those acts relate to a pattern of criminal activity or otherwise would cause a reasonable person to perceive a threat to DoD personnel, facilities, or forces in transit.

A7.10. Surveillance. Monitoring the activity of DoD personnel, facilities, processes, or systems, including showing unusual interest in a facility, infrastructure, or personnel (e.g., observation through binoculars, taking notes, drawing maps or diagrams of the facility, and taking pictures or video of a facility, infrastructure, personnel, or the surrounding environment) under circumstances that would cause a reasonable person to perceive a threat to DoD personnel, facilities, or forces in transit.

A7.11. Testing of Security. A challenge to, or a series of interactions with DoD installations, vessels, personnel, or systems that could reveal physical, personnel, or cyber security capabilities or vulnerabilities.

A7.12. Theft, Loss, or Diversion. Theft or loss associated with a DoD facility or infrastructure (e.g., of badges, uniforms, identification cards, emergency vehicles, technology, or documents, whether classified or unclassified) that are proprietary to the facility, or a diversion of attention from a DoD facility or infrastructure that is related to a theft or loss associated with that facility.

A7.13. Weapons Discovery. Discovery of weapons or explosives, as defined in Section 930 of Title 18, U.S.C. (Reference (n)). The discovery of personal weapons legally owned by DoD civilian employees, military members, or their dependents should not be reported as suspicious activity if the discovery is solely the result of the owner's failure to properly store, register, or secure the weapon(s).

A7.14. Unexplained Absences of International Military Students. International military students who are unexpectedly absent from scheduled activities when the absence is without proper authorization and lasts more than 24 hours, and an appropriate official with the host DoD organization determines that the absence is not due to a misunderstanding in scheduling, to sickness, or to another similar reason.

Attachment 8 (Added-30SW)

VISUAL AIDS

Figure A8.1. (Added) FPCON Normal Real World Visual Aid

Figure A8.2. (Added) FPCON Alpha Real-World Visual Aid

Figure A8.3. (Added) FPCON Alpha Exercise Visual Aid

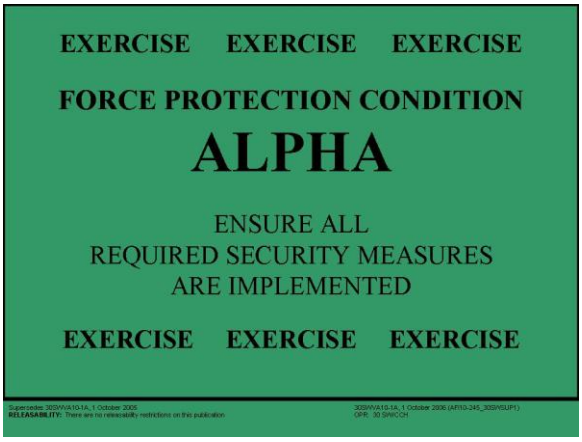


Figure A8.4. (Added) FPCON Bravo Real-World Visual Aid

Figure A8.5. (Added) FPCON Bravo Exercise Visual Aid

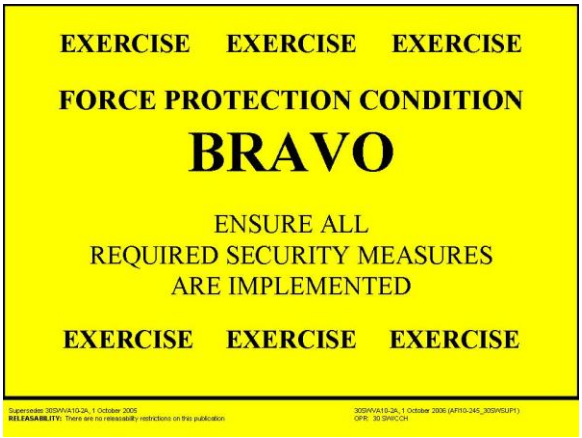


Figure A8.6. (Added) FPCON Charlie Real-World Visual Aid

Figure A8.7. (Added) FPCON Charlie Exercise Visual Aid

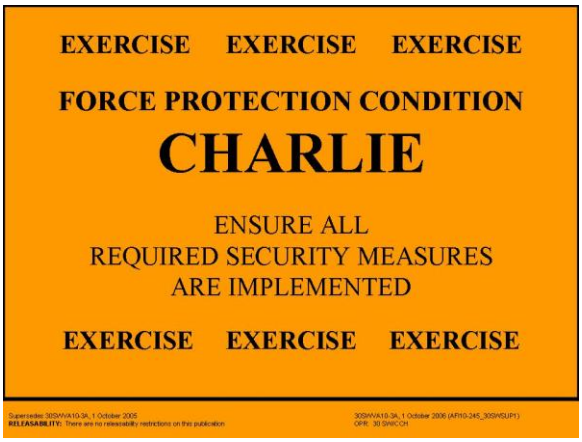


Figure A8.8. (Added) FPCON Delta Real-World Visual Aid

Figure A8.9. (Added) FPCON Delta Exercise Visual Aid

Figure A8.10. (Added) Bomb Threats Visual Aid

WARNING!

BOMB THREATS

STEPS TO TAKE

• ***Initiate*** AF Form 440, located by your phone, ask every question and follow all the steps
• Do ***not*** hang up the phone, it will make it easier to trace the call
• ***Call*** 911 on a different line
• ***STAY ON THE LINE*** until the dispatcher gives you the okay to leave. Responding forces need you to give the necessary information for their response
• Do not change the environment. Leave lights on if they were on, or leave them off if they were off. Do not use electrical devices (radios, cell phones, etc.)
• Evacuate the facility (Designated by the facility evacuation plan). Ensure the evacuation point is not in close proximity to the facility.
ENSURE the evacuation point is free from objects (cars, trash containers, etc.) in case a secondary device has been placed or hidden
• All pertinent personnel (911 caller, recipient of bomb threat) need to meet the responding forces once on scene with AF Fm 440 information and answer any question they may have in order to effectively diffuse the situation.

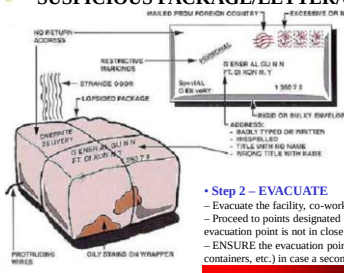
Dial 911

OPR: 30 SW/CCH
RELEASABILITY: There are no releasability restrictions on this publication.
30SWVA10-9, 15 December 2006 (Prescribed by: AFI10-245_30SWSUP)
Certified Current as of 11 February 2011

Figure A8.11. (Added) Suspicious Package/Letter /Unattended Items Visual Aid

WARNING!

SUSPICIOUS PACKAGE/LETTER/UNATTENDED ITEMS



• **Step 1 – DO NOT TOUCH ANYTHING**
– Do not handle the package/letter
– Do not accept a suspicious package/letter
– Do *not* change the environment. Leave lights on if they were on, or leave them off if they were off. Do not use electrical devices (radios, cell phones, etc.)
• BEFORE YOU LEAVE, Remember all the details (appearance, location, etc.) about the event to inform responding forces.

• **Step 2 – EVACUATE**
– Evacuate the facility, co-workers, people in immediate area
– Proceed to points designated on unit evacuation plan. Ensure the evacuation point is not in close proximity to the facility
– ENSURE the evacuation point is free from objects (cars, trash containers, etc.) in case a secondary device has been placed or hidden

Dial 911

– Call 911
– DO NOT USE a phone near the object
– Provide as much detailed info as possible - where, when, what, any details
– *More information is better than less!*
• All pertinent personnel (911 caller, discoverer of suspicious object) need to *meet* the responding forces on scene with information and answer any question they may have in order to effectively diffuse the situation

OPR: 30 SW/CCH
RELEASABILITY: There are no releasability restrictions on this publication.
30 SW VA 10-8, 15 December2006 (Prescribed by AFI10-245_30SWSUP)
Certified Current as of 11 February 2011

Figure A8.12. (Added) Suspicious Powder Or Substance Visual Aid

WARNING!

SUSPICIOUS POWDER OR SUBSTANCES

STEPS TO TAKE

1. Do not shake or empty the contents and try not to smell/inhale the substance.
2. Double bag (with gloves) or COVER the envelope or package with anything (e.g., clothing, paper, trash can, etc.)
3. LEAVE the room, CLOSE the door and prevent others from entering.
4. CALL 911

5. All persons in contact with substance WASH your hands with soap and water.

6. LIST all people who were in the room or area when this suspicious letter or package was recognized. Give this list to medical & law enforcement personnel.

7. Place all items worn at the time in plastic bags and keep them available for law enforcement. If possible change clothing in the workplace and DO NOT let anyone else touch the clothing.

8. If possible shower with soap and water.

9. Follow all instructions given by first responders.

Dial 911

OPR: 30 SW/CCH
RELEASABILITY: There are no releasability restrictions on this publication.
30 SW VA 10-8, 15 December2006 (Prescribed by AFI10-245_30SWSUP)
Certified Current as of 11 February 2011

Figure A8.13. (Added) Antiterrorism Memory Jogger Card

ANTITERRORISM/FORCE PROTECTION PROGRAM (AT/FP)

PURPOSE: To seek, deter, or blunt terrorist acts against USAF personnel and resources.

HOW: Through timely dissemination of threat information, creating awareness programs, and implementing defensive measures.

FORCE PROTECTION CONDTIONS (FPCON) DEFINITIONS

NORMAL: Applies when a general global threat of possible terrorist activity exists and warrants a routine security posture. At a minimum access control will be conducted at all DOD installation and facilities.

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 FPCON measures resulting from intelligence received or as a deterrent. The measures in this FPCON must be capable of being maintained indefinitely.

BRAVO: Applies when an increased or more predictable threat of terrorist activity exists. Sustaining BRAVO measures for a prolonged period may affect operation capability and military-civil relationships with local authorities

CHARLIE: Applies when an incident occurs or intelligence is received indicating that some form of terrorist action or targeting against personnel or facilities is likely. Prolonged implementation of CHARLIE measures may create hardship and affect the activities of the unit and its personnel.

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. FPCON DELTA is usually declared as a localized condition. FPCON DELTA measures are not intended to be sustained for an extended duration.

TERRORISM DEFINED: The calculated use of unlawful violence or threat of unlawful violence to include fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

Supersedes: 30SWVA10-6, 18 November 2008 30 SW VA 10-6, 15 December 2006
(Prescribed by AFI10-245_30SWSUP) **Certified Current as of 11 February 2011**
RELEASABILITY: There are no releasability restrictions on this publication OPR: 30 SW/CCH

THREAT AWARENESS MEMORY JOGGER

- CONSTANTLY BE AWARE OF YOUR SURROUNDINGS. Know the terrorist threat levels for your duty or TDY locations. Contact your supervisor, commander, or local AFOSI DET for this information.

REPORT SUSPICIOUS ACTIVITY TO THE SECURITY FORCES AT 911.

- BE PREPARED TO PROVIDE A FULL DESCRIPTION OF THE INCIDENT (Use the SALUTE Format. Size, Activity, Location, Uniform, Time, and Equipment)
- DEVELOP A PERSONAL THREAT AWARENESS SECURITY CHECKLIST—Key on areas of residence, transportation, personal, mail handling, and duty location
- ENSURE AVENUES OF APPROACH ARE CLEAR AN ILLUMINATED—Lock doors and windows, stop mail and deliveries when TDY or on leave
- VARY YOUR ROUTES OF TRAVEL AT BOTH ORIGIN AND DESTINATION AND USE HEAVILY TRAVELED ROUTES—KNOW SAFE HAVENS—INSTALL AN ALARM
- DEVELOP A FAMILY VERBAL CODE SYSTEM FOR ALERTING DANGER OR REQUEST FOR HELP—Always question the suspicious—Travel in small groups when possible
- NEVER ACCEPT MAIL THAT DOES NOT COME THROUGH THE POSTAL SYSTEM—Look for unusual postmarks, presence of a return address, misspellings, non-specific addresses, excessive postage, abnormal weight and size, stains, wires, or strings, bulges, or lopsided letters
- IMPLEMENT LOCAL FORCE PROTECTION CONDITION MEASURES FULLY—Control and escort visitors, control access to work centers—Never be complacent in your duties

Supersedes: 30SWVA10-6, 18 November 2008 30 SW VA 10-6, 15 December 2006
(Prescribed by AFI10-245_30SWSUP) **Certified Current as of 11 February 2011**
RELEASABILITY: There are no releasability restrictions on this publication OPR: 30 SW/CCH