

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

AIR FORCE INSTRUCTION 10-245



25 JUNE 2015

**AIR FORCE MATERIAL COMMAND
Supplement**

15 AUGUST 2016

Operations

ANTITERRORISM (AT)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing web site at www.e-Publishing.af.mil

RELEASABILITY: There are no releasability restrictions on this publication

OPR: AF/A4SO

Certified by: AF/A4S
(Brig Gen Allen J. Jamerson)

Pages: 104

Supersedes: AFI 10-245,
21 September 2012

(AFMC)

OPR: HQ AFMC/A4SA

Certified by: HQ AFMC/A4S
(Colonel Thad B. Hill)

Pages: 17

Supersedes: AFI 10-245_AFMCSUP,
30 October 2014

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 DoDI 2000.12, *DoD Antiterrorism (AT) Program*; DoDI 3020.45, *Defense Critical Infrastructure Program (DCIP) Management*; DoDI 6055.17, *DoD Installation Emergency Management (IEM) Program*; DoDI 6200.03, *Public Health Emergency Management Within the Department of Defense*; Air Force Doctrine Annex 3-10, *Force Protection*; Air Force Doctrine Annex 4-0, *Combat Support*; AFPD 31-1, *Integrated Defense*; AFPD 10-25, *Emergency Management*; AFPD 10-24, *Air Force Critical Infrastructure Program (CIP)*; AFPD 10-26, *Counter-Chemical, Biological, Radiological, and Nuclear Operations*; AFPD 10-39, *Safeguarding Biological Select Agents and Toxins*; and Air Force Instruction (AFI) 16-1402, *Insider Threat Program Management*. It establishes responsibilities and guidance for the Air Force (AF) Antiterrorism Program. This 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. The authorities to waive wing/unit level requirements in this publication are identified with a Tier (“T-0, T-1, T-2, T-3”) number following the compliance statement. See AFI 33-360, *Publications and Forms Management*, Table 1.1 for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the Publication OPR for non-tiered compliance items. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW Air Force Manual (AFMAN) 33-363, Management of Records, and disposed of IAW the Air Force Records Disposition Schedule (RDS) in the Air Force Records Information Management System (AFRIMS). This publication may be supplemented at any level, but all direct Supplements must be routed to the OPR of this publication for coordination prior to certification and approval. Supplementary guidance (which includes supplements and separate publications) cannot be less restrictive than the parent publication, but it can be more restrictive. 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 Forms 847 from the field through the appropriate functional chain of command. 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.

(AFMC) This supplement implements AFI 10-245, Antiterrorism (AT), 25 June 2015. It expands on the guidance in the Air Force Instruction, delineates specific responsibilities, and applies to AFMC controlled installations, complexes, plants, labs, sites, and stand-alone facilities (hereafter referred to as installations), within AFMC to include all units assigned and/or attached to AFMC, Government-Owned, Contractor-Operated (GOCOs) IAW binding agreements or obligations with the Department of the Air Force. For specific GOCO requirements refer to the Security and Antiterrorism Requirements section in the Lease Clause of each GOCO agreement, AFI 31-101_AFMCSUP, Chapter 14, and local Memorandums of Understanding related to Security and Antiterrorism. Tenants on AFMC installations will participate in the host installation antiterrorism program as stated in the host/tenant agreement. The terms “must,” “shall,” and “will” denote mandatory actions in this supplement. IAW AFI 33-360, Publications and Forms Management, the authorities to waive wing/unit level requirements are identified with a Tier (“T-0, T-1, T-2, T-3”) number following the compliance statement. Requests for waivers must come from the commanders (or civilian directors) of the affected unit seeking relief from compliance through the command chain up to the appropriate tier approval authority (i.e., Tier 0, 1, 2, 3) or publications approval authority if non-tiered. Send comments and suggested improvements on AF Form 847, Recommendation for Change of Publication, through unit force protection channels to HQ AFMC/Security Forces, Building 266, room A108, 4225 Logistics Avenue, Wright-Patterson AFB OH 45433-5760. This instruction does not apply to the US Air Force Reserve or Air National Guard. The manual may be supplemented at any level, but all supplements must be routed to HQ AFMC/Security Forces for coordination prior to certification and approval. All waiver requests must be routed to the OPR for approval prior to implementation. 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 Information Management System (AFRIMS) Records Disposition Schedule (RDS).

SUMMARY OF CHANGES

All installation-level and below requirements have been tiered in accordance with AFI 33-360, *Forms and Publications Management*. The requirement for designating Antiterrorism Officers and Antiterrorism Representatives (ATRs) has been clarified. Additionally, training requirements for ATRs have been defined.

(AFMC) Removal of all non-directive guidance and guidance that did not add validity to the supplement; Critical Asset List (CAL) utilization to develop other installation priority response list; tiering of additional paragraphs; addition of AFNORTH (AFNI) 10-222, *Force Protection (FP) Mission and Antiterrorism (AT) Program for Air Forces Northern Area of Responsibility* guidance; update of HQ AFMC Antiterrorism Working Group (ATWG) membership IAW new organization construct; clarified Antiterrorism Officer (ATO)/Antiterrorism Representative (ATR) rank requirements if an installation/unit is unable to meet rank requirements; rank and duty position requirements for Threat Working and Antiterrorism working groups; and mandatory unit development of site-specific FPCON measures.

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.	8
1.4. AT Program Roles and Responsibilities.	9
Chapter 2—ANTITERRORISM STANDARDS	23
2.1. Standard 1:	23
2.2. Standard 2:	23
2.3. Standard 3:	24
Figure 2.1. AT Risk	25
2.4. Standard 4:	25
2.5. Standard 5:	26
2.6. Standard 6:	27
2.7. Standard 7:	31
Table 2.1. AT Threat Planning Scenarios	33
2.8. Standard 8:	35
2.9. Standard 9:	36
2.10. Standard 10:	40
2.11. Standard 11:	41
2.12. Standard 12:	42

2.13.	Standard 13:	43
2.14.	Standard 14:	44
2.15.	Standard 15:	45
2.16.	Standard 16:	46
2.17.	Standard 17:	47
2.18.	Standard 18:	48
2.19.	Standard 19:	49
2.20.	Standard 20:	49
2.21.	Standard 21:	49
2.22.	Standard 22:	51
2.23.	Standard 23:	52
2.24.	Standard 24:	53
2.25.	Standard 25:	53
Table 2.2.	Level I - AT Awareness Training Requirements	55
2.26.	Standard 26:	55
Table 2.3.	Level II – ATO Training Requirements	57
Table 2.4.	ATR Training should include the following topics	57
2.27.	Standard 27:	58
Table 2.5.	Level III - Pre-Command AT Training Requirements	59
2.28.	Standard 28:	59
2.29.	Standard 29:	59
2.30.	Standard 30:	60
2.31.	Standard 31:	61
2.32.	Standard 32:	62
Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION		63
Attachment 2—FORCE PROTECTION CONDITION (FPCON) MEASURES		79
Attachment 3—TERRORIST THREAT LEVELS		90
Attachment 4—RISK MANAGEMENT AND RESOURCING PROCESSES		92
Attachment 5—AF APPROVED LEVEL II - ATO CERTIFICATION TRAINING COURSES		94
Attachment 6—THE ANTITERRORISM STANDARDS FOR BUILDINGS DEVIATION PROGRAM		95

AFI10-245_AFMC SUP 15 AUGUST 2016	5
Attachment 7—CATEGORIES OF SUSPICIOUS ACTIVITY	99
Attachment 8—(Added-AFMC) UNIT PROGRAM REVIEW (UPR)	101
Attachment 9—(Added-AFMC) ANTITERRORISM APPOINTMENT LETTER TEMPLATE (INSTALLATION ATO)	103
Attachment 10—(Added-AFMC) ANTITERRORISM APPOINTMENT LETTER TEMPLATE (WING ATO/UNIT ATR)	104

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's 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 information 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.

1.1.1. **(Added-AFMC)** This supplement establishes Major Command (MAJCOM) guidance and procedures for implementing the DoD Antiterrorism (AT) Program, the Air Force (AF) AT Program, the United States Northern Command (USNORTHCOM) Force Protection (FP) AT Program, and 1 AF (AFNORTH) Force Protection (FP) Mission and Antiterrorism (AT) Program for Air Force Northern Area of Responsibility and applies to AFMC controlled installations, complexes, plants (as required by contractual obligations), labs, sites, and stand-alone facilities (hereafter referred to as installations). AFMC installations that fall under the responsibilities of other Geographic Combatant Commanders (GCC) (not USNORTHCOM) and/or are supported by other installations will follow the owning GCC/supporting installation requirements, when they conflict with USNORTHCOM/AFNORTH/AFMC guidance, inform HQ AFMC/A4S. (T-2)

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 to mitigate or accept any AT risk that cannot be controlled to an acceptable level within a commander's resources **(T-1)**.

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.

1.2.1. **(AFMC)** Requirements and/or tasks for installations, mandated by this supplement, shall flow through the respective Centers as required (T-3).

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 MAJCOM or installation, and coordinate the efforts of key functional

areas to ensure synergy on behalf of the commander (**T-0**). At a minimum, Security Forces, Air Force Office of Special Investigations (AFOSI), Intelligence, Civil Engineers (to include Emergency Management, Explosive Ordnance Disposal (EOD) and Fire Emergency Services), Force Support, Command Post, Information Protection, Critical Asset Risk Management (CARM) Program Manager, Public Affairs, Cyberspace Operations, Contracting, Operations, Medical (to include Public Health, Bioenvironmental Engineering (food and water) and Medical Treatment Facility Emergency Manager (MEM)), Judge Advocate, and Comptroller must coordinate efforts to achieve an effective AT posture. The installation ATO is responsible for coordinating among these key players and facilitating the integration of their efforts on behalf of the commander. As a sub-element of the overarching force protection program (FP), 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 should maintain awareness of potential terrorist and insider 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 (**T-3**). If agreements with outside agencies do not provide sufficient support to the AT program, associated vulnerabilities will be entered into the Core Vulnerability Assessment Management Program (CVAMP) explaining the lack of support (**T-2**).

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 (**T-1**).

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 dependents. The Eagle Eyes program will inform the community on how to recognize possible terrorist activity and how to report suspicious behavior (**T-1**). 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.

1.2.5.1.1. (**Added-AFMC**) AFOSI provides threat data to the Installation Commander or vice and/or the Defense Force Commander (DFC) as appropriate to ensure an optimal common operating picture and an Antiterrorism/Integrated Defense

(AT/ID) posture for the given installation's Area of Responsibility (AOR) IAW AFMD 39 and AFPD 71-1. (T-2)

1.2.5.1.2. **(Added-AFMC)** Installations will take advantage of multi-media venues to inform the installation beneficiary population about the Eagle Eyes program. The Eagle Eyes template for local production and distribution to the base and local civilian community as appropriate is located at <http://www.osi.af.mil/eagleeyes/> along with AFOSI's "Crimebusters" link for direct e-mail notification to the HQ AFOSI Watch (24/7). AFOSI also promotes community's involvement in security through local public affairs through base newspapers. Additionally, if a reporter prefers to remain anonymous, they can use the AFOSI anonymous tip line by visiting <https://www.tipsubmit.com/WebTips.aspx?AgencyID=1111> or download the TipSubmit Mobile application from your provider's marketplace - Select "Federal/Military" and then "Air Force Office of Special Investigations" or text "AFOSI" plus your tip information to 274637 (CRIMES). The AFOSI Tip Line provides service members and civilians a safe, discreet and anonymous option to report criminal information, counterintelligence indicators or force-protection concerns. (T-2).

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 **(T-0)**. MAJCOM ATPM, installation ATO, and authorized members of the Intelligence Fusion Cell (IFC) will have read access to the eGuardian system **(T-0)**. 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.

1.2.5.2. **(AFMC)** These procedures shall be included in either the installation's AT Plan or Integrated Defense Plan (IDP) (T-3).

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 **(T-0)**. 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.

1.3.1.1. **(Added-AFMC)** AFMC and subordinates will follow guidance laid out in USNORTHCOM Instruction (NCI) 10-222, *USNORTHCOM Force Protection Mission*

and Antiterrorism Program (T-2) and AFNORTH (AFNI) 10-222, Force Protection (FP) Mission and Antiterrorism (AT) Program for Air Forces Northern Area of Responsibility.

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 (**T-0**). 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 (**T-0**).

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) (**T-0**). AF personnel in-transit on Leave/Temporary Duty (TDY) or deployment orders shall also comply with Standard 29 of this AFI.

1.3.3.1. (**Added-AFMC**) Installation commanders will establish and annually review their "Overseas Travel Policy" (T-2). It will address at a minimum; travel to high risk areas, AT Level I training, review of the Foreign Clearance Guide (FCG), security responsibilities, risk assessment process, travel itineraries and procedures for reporting suspicious activity (T-2).

1.3.3.2. (**Added-AFMC**) Travelers will review and ensure Aircraft and Personnel Automated Clearance System (APACS), <https://apacs.dtic.mil/apacs/> travel clearance requests are submitted within the required lead-time and with all required content/documents (T-2).

1.3.3.3. (**Added-AFMC**) Commanders, at all levels, shall establish a process to ensure unit members are briefed on foreign travel restrictions and Combatant Commander-established country entry requirements before departing outside the Continental United States (OCONUS) deployments or approving OCONUS leaves (T-2).

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]) (**T-1**).

1.4.1.1.1. **(Added-AFMC)** When supplemented, installation commanders or civilian equivalent will provide HQ AFMC Security Forces with a copy of their supplement to AFI 10-245 within 30 days of approval. Provide a copy of your supplement in the appropriate folder on EIM <https://cs.eis.afmc.af.mil/sites/AT-FP/AFMC%20Installations/Forms/AllItems.aspx> and notify the HQ AFMC/A4S (T-2).

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 **(T-0)**.

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 **(T-0)**.

1.4.1.3.1. **(Added-AFMC)** AFMC Centers (except for AFIMSC) are in the direct chain-of-command for AFMC installations, labs, plants, and sites and as such, are required to have active AT Programs. (T-2)

1.4.1.3.2. **(Added-AFMC)** Installation Commander, at a minimum, will brief (e.g., telecon, VTC, MFR, face-to-face, etc.) semi-annually the Center Commander on AT matters affecting their installations (e.g., CVAMP Vulnerability/Concern/UFR status and command observation trend analysis, HQ assessments, FPCON changes, threats affecting mission capabilities, AT waiver packages, etc.) (T-2).

1.4.1.4. GSUs attached to an installation will be included in the installation AT Plan and comply with all installation AT program requirements **(T-0)**. Installation Commanders shall ensure coordination on AT program elements and responsibilities regarding GSUs **(T-2)**.

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 support, 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). Particular care must be taken regarding the collection, retention, or dissemination of intelligence information on US persons, in CONUS or OCONUS. These activities are highly regulated and must comply with DoD 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons*, and Executive Order 12333, *United States Intelligence Activities*.

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 Security Enterprise and Mission Assurance (SE/MA) Working Group, and HAF SE/MA Steering Group 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. Air Force Office of Special Investigations (AFOSI). AFOSI shall provide counterintelligence (CI) and criminal investigative support to the AT program. Reference AFPD 71-1, *Criminal Investigations and Counterintelligence*, and AFI 71-101 Volume 4, *Counterintelligence*.
 - 1.4.2.2.1. AFOSI/JA shall provide legal advice and guidance for all Counterintelligence antiterrorism investigations and operations. AFOSI/JA is the primary legal office authorized to provide legal guidance and conduct legal reviews of specialized techniques conducted by AFOSI.
 - 1.4.2.2.2. All specialized techniques must be reviewed for legal sufficiency prior to operation initiation. Procedures requiring approval outside AFOSI will be staffed through HQ AFOSI to SAF/GC. The request will be reviewed by SAF/GC who will ensure approval is obtained from the appropriate authority.
 - 1.4.2.2.3. Conduct counterintelligence (CI) activities, to include operations, investigations, collections, services, production, and analysis of threats from terrorism.
 - 1.4.2.2.4. 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.
 - 1.4.2.2.5. Provide warning of potential terrorist or unconventional warfare activities that are threats to Department of the Air Force personnel, property or assets worldwide.
 - 1.4.2.2.6. Provide personal protective services for senior US, DoD, Air Force and allied officials.
 - 1.4.2.2.7. Manage the USAF Non-Tactical Armored Vehicle Program.
 - 1.4.2.2.8. Assist in the provision of AT training, to include the HRP training required by Standard 16.
 - 1.4.2.2.9. Provide an AFOSI focal point to the Air National Guard.
- 1.4.2.3. The 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 SE/MA Working Group and HAF SE/MA Steering Group 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 or 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 Public Health Emergency Management 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 AFMAN 10-246, *Food and Water Protection Program*. Coordinate food, water, toxic industrial chemical and toxic industrial material vulnerability assessments (VA) with AT VAs at all levels and ensure reports facilitate CVAMP format/entries.

1.4.2.5.3. Ensure appropriate aspects of the AT Program are integrated with the Public Health Emergency Management Program as defined in AFPD 10-26, and AFI 10-2603, *Emergency Health Powers on Air Force Installations*.

1.4.2.6. Chief of 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, 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 in accordance with Standard 24, DODI 2000.16.

1.4.2.8. Deputy Chief of Staff, 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 policies affecting intelligence support to the AT mission.

1.4.2.8.3. Represent the Air Force in Director of National Intelligence (DNI), DoD and Intelligence Community venues on matters of intelligence and collaborate with HQ AFOSI (SAF/IGX) and AF/A4S on AT information, policy, processes and assessments.

1.4.2.9. Deputy Chief of Staff, Operations (AF/A3). AF/A3 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 Defense Critical Infrastructure Program (DCIP) and AF requirements.
 - 1.4.2.9.4. Ensure AT is factored into operational plans.
 - 1.4.2.9.5. 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). AF/A4 is the OPR for Air Force AT policy, guidance, and instruction. AF/A4 shall:
- 1.4.2.10.1. Through AF/A4S:
 - 1.4.2.10.1.1. Draft and coordinate policy and guidance with the HAF SE/MA Working Group and HAF SE/MA Steering Group 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 code (PEC) 28047F and coordinate funding for AT initiatives with Air Staff functional experts for AF/A4 approval.
 - 1.4.2.10.1.4. Evaluate AT non-medical 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 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 Standard 18.
 - 1.4.2.10.2.5. Incorporate AT considerations in the expeditionary support planning program.
 - 1.4.2.10.3. Through AF/A4C:
 - 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. Implement the crisis and consequence management aspects of homeland defense and civil support, and the non-medical CBRN defense elements 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 provide a member to the HAF SE/MA Working Group and HAF SE/MA Steering Group.

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

1.4.2.11. Chief, Information Dominance and Chief Information Officer(SAF/CIO A6). SAF/CIO A6 shall:

1.4.2.11.1. Provide AF policy and guidance to enable an operationally-resilient, reliable and secure cyberspace domain to meet AT mission needs 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 Requirements (AF/A5/8). AF/A5/8 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 and Assessments (AF/A9). AF/A9 shall provide appropriate studies and AT lessons learned from exercises and actual operations and events.

1.4.2.14. Assistant Chief of Staff, Strategic Deterrence and Nuclear Integration (AF/A10). AF/A10 shall:

1.4.2.14.1. Ensure that AT standards are maintained or exceeded in nuclear security standards and requirements, and Countering Weapons of Mass Destruction (C-WMD) standards and requirements.

1.4.2.14.2. Provide guidance and expertise on those aspects of AT related to Counter-Chemical, Biological, Radiological, and Nuclear (C-CBRN) and Countering WMD operations IAW AFD 10-26 and AFD 10-39.

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.

1.4.3.1.1. **(Added-AFMC)** Centers are responsible for implementing DOD, USNORTHCOM, AFNORTH, HAF and AFMC AT policy within their organization and subordinate units.

1.4.3.2. MAJCOM ATPMs shall oversee funds provided in PEC 28047F 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. Consider combining/including other related working groups and councils as appropriate.

1.4.3.3. **(AFMC)** In accordance with PAD 14-04, Annex T AFIMSC Det 6, in coordination with HQ AFMC/A4S Senior FP Advisor, will lead day-to-day program management of all risk-managed working groups at the MAJCOM level. (T-2)

1.4.3.3.1. **(Added-AFMC)** Management of FP risk understanding and acceptance.

1.4.3.3.2. **(Added-AFMC)** Recommend actions for FP risks to installations and deploying forces.

1.4.3.3.3. **(Added-AFMC)** Plan and task FP operational requirements.

1.4.3.3.4. **(Added-AFMC)** The Corporate Readiness Structure incorporates six working groups (WGs) as part of the Readiness Board structure: Exercise and Evaluation Program Working Group (EEPWG), Expeditionary Skills Working Group (ESWG), Antiterrorism Working Group (ATWG); Emergency Management Working Group (EMWG), Critical Asset Risk Management Working Group and Counter-Chemical, Biological, Radiological, Nuclear Working Group (C-CBRN WG). The Readiness Council fulfills the requirements of an ATEC as is led by AFIMSC Det 6.

1.4.3.3.5. **(Added-AFMC)** The HQ AFMC ATWG consists of representatives from Intelligence (A2), Operations (A3), Logistics (A4 – Civil Engineers (A4C), Readiness (A4R) and Security Forces (A4S), Communications (A6), , Strategic Plans and Programs (A8), Lessons Learned (A9), Information Protection (IP), Judge Advocate (JA), Public Affairs (PA), Safety (SE), Surgeon General (SG), AFIMSC Det 6 (Civil Engineers and Security Forces), and AFOSI (non-staff FOA). They are HQ AFMC/CC's advisory body on AT policy and program management. The ATWG is charged with the overall effectiveness of the command's force protection program. AFIMSC Det 6 will serve as Chairperson of the ATWG. (T-2)

1.4.3.3.6. **(Added-AFMC)** AFIMSC, Det 6 will provide at least one member to the ATWG that has been to the Security Engineering Design Course, one EOD, one Fire, one Emergency Management, and one Security Forces SME to support the ATWG. (T-2)

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.

1.4.3.6. **(Added-AFMC)** AFIMSC, Det 6/Civil Engineer will coordinate with the HQ AFMC/A4S on all new and major renovations, modifications, repairs, revitalizations, and restorations that meet the triggering requirements as outlined in UFC 4-010-01, *DoD Minimum Building Standards*, to ensure the minimum building standards are met. (T-2)

1.4.3.7. **(Added-AFMC)** In accordance with PAD 14-04, Annex T AFIMSC Det 6 will lead day-to-day program management of the Vulnerability Prioritization Program for AFMC. (T-2)

1.4.3.7.1. **(Added-AFMC)** Manage measures taken to mitigate hostile actions against personnel (to include family members), resources, and facilities.

1.4.3.7.2. **(Added-AFMC)** Request waivers for FP and threat mitigation requirements for AFMC/CC approvals.

1.4.3.7.3. **(Added-AFMC)** Serve as FP liaison to CCDR, other DoD, Interagency, and Host Nation authorities for the cross-flow of information on FP issues and threats.

1.4.3.7.4. **(Added-AFMC)** Manage vulnerability oversight which includes managing, tracking, prioritizing, and mitigating vulnerabilities using CVAMP IAW AFMC/CC priorities. Vulnerability prioritization program management must be closely coordinated with the HQ AFMC/A4S due to the complementary nature of this program with Integrated Defense, as prescribed in AFPD 31-1.

1.4.3.7.5. **(Added-AFMC)** Manage travel to AOR travel-restricted areas.

1.4.3.7.6. **(Added-AFMC)** Oversee the Core Vulnerability Assessment Management Program (CVAMP).

1.4.4. Installations:

1.4.4.1. AT is an installation commander's responsibility and must be thoroughly integrated into every unit attached to the installation, to include tenants, sister services, and attached agencies. The installation commander will appoint the Defense Force Commander as the installation ATO **(T-1)**.

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 **(T-0)**. To optimize force protection capabilities, installations may also combine the ATWG, IDWG, Emergency Management Working Group (EMWG), and other related working groups into a single working group. The ATEC should be combined with the Integrated Defense Council (IDC).

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 Squadron (FSS) Commanders 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 **(T-2)**.

1.4.4.4.1. **(AFMC)** Ensure all local assessments are coordinated with the installation ATO **(T-3)**.

1.4.4.4.2. Assist in the review of Air Force Manpower Standards and manpower determinant tools for appointed AT positions as described in AFI 38-201, *Management of Manpower Requirements and Authorizations* **(T-3)**.

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. **(T-3)**.

1.4.4.5. Contracting Squadron (CONS) Commanders 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 in compliance **(T-0)**. 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 **(T-0)**. 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 **(T-3)**.

1.4.4.5.4. Coordinate necessary background investigations for contractors with the installation Information Protection office and work with the Defense Force Commander to develop mitigation measures that limit the potential for terrorist and insider threats posed by contractors while on the installation **(T-0)**.

1.4.4.5.5. Incorporate AT clauses required by DFARS, related supplements, and local AT measures as part of requirements for DoD contracts, as described in DoDI 2000.16, Standard 18 **(T-0)**.

1.4.4.6. Communications Squadron (CS) Commanders 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 in Enterprise Mission Assurance Support System (eMASS) in accordance with AFI 33-210 **(T-1)**. The information system vulnerability must be tracked until resolved and documented in the Plan of Actions & Milestones approved by the Authorizing Official **(T-1)**.

1.4.4.6.2. Implement AT policy and guidance for mail handling and management **(T-2)**.

1.4.4.6.2.1. **(Added-AFMC)** Policy and guidance shall include the following: **(T-2)**

1.4.4.6.2.1.1. **(Added-AFMC)** HVAC shutdown procedures.

1.4.4.6.2.1.2. **(Added-AFMC)** Response actions to suspicious envelope(s) or package(s).

1.4.4.6.2.1.3. **(Added-AFMC)** Evacuation points for non-contaminated/contaminated employees.

1.4.4.6.2.1.4. **(Added-AFMC)** Notifying emergency responders.

1.4.4.6.2.1.5. **(Added-AFMC)** Notifying facility occupants.

1.4.4.6.2.1.6. **(Added-AFMC)** Isolating suspicious envelope(s) and package(s).

1.4.4.6.2.1.7. **(Added-AFMC)** Type and proper use of Individual Protective Equipment (IPE).

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 **(T-2)**.

1.4.4.6.4. **(Added-AFMC)** Develop training aids to properly exercise mail handling procedures. (e.g., x-ray machines, explosive detectors, suspicious packages, etc.).

1.4.4.7. Comptroller Squadron (CPTS) Commanders shall:

1.4.4.7.1. Assist in building budget submissions to obtain AT funding (PEC 28047F) for validated AT projects **(T-3)**.

1.4.4.7.1. **(AFMC)** Work with installation ATO and the Base Civil Engineer (BCE) to ensure sustainment and/or preventive maintenance costs for AT security requirements are incorporated into funding requests. (T-3)

1.4.4.7.2. Work with the installation ATO to validate funding issues in CVAMP and Automated Civil Engineering System (ACES) **(T-3)**.

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 **(T-3)**.

1.4.4.8. Unit Intelligence 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 **(T-2)**.

1.4.4.8.2. Designate intelligence personnel to participate in ATWGs, TWGs, and other force protection-associated programs and functions (e.g., IDWG and IFC), as appropriate **(T-2)**.

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 **(T-2)**.

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. Partner with AFOSI to:

1.4.4.8.5.1. Analyze all-source intelligence information for impact on unit mission and rapidly disseminate terrorist or insider threat information to subordinate and lateral units, HHQs and other appropriate agencies **(T-2)**. Such dissemination must comply with controlling guidance on dissemination of information concerning US persons **(T-0)**.

1.4.4.8.5.2. Establish procedures to track DoD Terrorism 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) **(T-2)**.

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 terrorists or insiders.

1.4.4.8.5.4. Support the annual development of the AFOSI Local Threat Assessment (LTA) and other threat assessments, as applicable **(T-2)**.

1.4.4.8.5.5. Any Air Force intelligence units supporting AT plans or other activities will comply with collection, retention, and dissemination restrictions on performing activities relating to US persons, which are included within DoD 5240.1-R, Executive Order 12333, and other applicable guidance and laws **(T-0)**.

1.4.4.9. Staff Judge Advocate shall:

1.4.4.9.1. Provide legal advice and guidance to the AT program **(T-2)**.

1.4.4.9.2. Review all new support agreements such as MOUs, MOAs, or MAAs needed to support the AT program for legal sufficiency. Thereafter, review support agreements IAW AFI 25-201, *Intra-Service, Intra-Agency, and Inter-Agency Support Agreement Procedures* **(T-1)**.

1.4.4.10. Security Forces Squadron (SFS) Commanders shall:

1.4.4.10.1. Ensure ID incorporates AT standards and contributes to installation AT planning **(T-3)**.

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 **(T-1)**.

1.4.4.10.3. The Security Forces Commander is also referred to as the Defense Force Commander throughout this instruction and is responsible for all aspects of installation physical security and resource protection programs, as part of the overall Integrated Defense effort and codified in the Integrated Defense Plan (IDP).

1.4.4.10.4. Plan for random antiterrorism measures (RAM) to counter threats, mitigate vulnerabilities and reduce risk **(T-3)**.

1.4.4.10.5. Present risk management analysis to the ATWG and ATEC (or other related working groups and councils as appropriate) to manage risk and appropriately adjust the protection posture of DoD elements and personnel **(T-3)**.

1.4.4.11. Civil Engineer Squadron (CES) Commanders 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 and projects supporting vulnerabilities identified in CVAMP are referenced and prioritized in ACES **(T-3)**.

1.4.4.11.1.1. **(Added-AFMC)** Ensure CVAMP tracking numbers is used when inputting related projects into ACES. Consequently, associated ACES' project numbers will be inputted into CVAMP observations. (T-2)

1.4.4.11.1.2. **(Added-AFMC)** When appropriate, ensure sustainment and/or preventive maintenance costs for physical security requirements are incorporated into overall project costs.

1.4.4.11.2. Implement terrorism incident planning for incident response, consequence management, and recovery, in coordination with the DFC **(T-0)**.

1.4.4.11.3. Provide engineering infrastructure protection expertise to counter and mitigate terrorist threats **(T-2)**.

1.4.4.11.4. Develop and maintain the installation barrier plan in coordination with appropriate agencies or ATWG **(T-3)**.

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 the installation planning team. The specific membership of a planning team will be based on local considerations, but in general, should consist of programmers, the installation ATO, and members of the Threat Working Group **(T-0)**.

1.4.4.11.6. Provide structural blast analysis using the Vulnerability Assessment Protection Option (VAPO) program for all facilities housing CARM Tier I and II critical assets **(T-1)**.

1.4.4.11.7. Develop and publish an All-Hazards Threat Assessment through the Emergency Management Working Group (EMWG) **(T-0)**.

1.4.4.11.8. Serve as the installation lead for conducting an annual CBRN and Explosive Hazard (EH) vulnerability assessment **(T-2)**. Ensure vulnerabilities and observations are entered in CVAMP within 90 days of the signed assessment report **(T-3)**. Monitor, track and manage these vulnerabilities until resolved by mitigation or installation commander's documented acceptance of risk (T-1).

1.4.4.11.9. **(Added-AFMC)** Ensure coordination with the installation ATO prior to scheduling and conducting local assessments.

1.4.4.11.10. **(Added-AFMC)** The CE representative will submit and manage UFC deviations, per Atch 6 and Standard 17, AT Construction and Building Considerations (T-2). All AT deviations will be coordinated with the installation ATO (T-2).

1.4.4.11.10.1. **(Added-AFMC)** Document deviations on AF Form 116, *Request for Deviation from Security Criteria*, and submit each deviation for formal

approval. Forward a copy of the AF Form 116, to the installation ATO. Upon formal approval by the MAJCOM CV, the AF Form 116 will be maintained by CES. (T-2)

1.4.4.11.10.2. **(Added-AFMC)** Ensure the installation ATO is chartered as an advisory member of all CE planning venues (e.g. pre-design charrette, Work Order Review Boards, Facility Utilization Boards, etc.).

1.4.4.12. Medical Group (MDG) Commanders shall:

1.4.4.12.1. Provide medical specialists (MEM, Public Health and Bioenvironmental Engineering) to the ATWG and ATEC for AT planning and assessments **(T-3)**.

1.4.4.12.2. Serve as the installation lead for conducting annual TIC/TIM and Food/Water VAs **(T-3)**. Ensure vulnerabilities and observations are entered in CVAMP within 90 days of the signed assessment report **(T-3)**. Monitor, track, manage and incorporate vulnerabilities into situational awareness and data analytical tools until resolved by mitigation or installation commander's documented acceptance of risk **(T-2)**. Ensure assessment reports are formatted for entry into CVAMP **(T-3)**.

1.4.4.12.3. Ensure local assessments per AFMAN 10-246 are consolidated and conducted at the same time as the local AT Vulnerability Assessment **(T-3)**.

1.4.4.13. Installation CARM Manager shall:

1.4.4.13.1. Integrate and synchronize CARM risk management requirements utilizing data systems and processes such as AF Critical Asset Management System (AF-CAMS) and the DCIP Assessment with the installation AT program **(T-1)**.

1.4.4.13.1. **(AFMC)** Ensure coordination with the installation ATO prior to scheduling and conducting local assessments.

1.4.4.13.2. Share all threat and hazard planning information and CARM Tier I (including Defense Critical Assets) and Tier II critical asset-related data to support the DFC's overall IDRMP **(T-0)**.

1.4.4.13.2. **(AFMC)** Coordinate with SFS to ensure Defense Critical Assets (DCAs), Task Critical Assets (TCAs) Tier I-III and Tasked Assets (TAs) are included and identified into the ForcePRO software.

1.4.4.13.3. Coordinate through installation working groups and the installation commander to the respective MAJCOM CARM managers in nominating and scheduling CARM Assessments for Tier I-II assets **(T-0)**.

1.4.4.13.4. Provide other support as outlined in this AFI.

1.4.4.14. Chief of Public Affairs shall:

1.4.4.14.1. Provide communications advice and counsel to those in charge **(T-3)**.

1.4.4.14.2. Establish procedures to handle crisis communications issues **(T-3)**.

1.4.4.14.3. Screen information disseminated to the media to ensure operational security and force protection **(T-3)**.

1.4.4.14.4. Provide procedures for the proper release of information during crises (T-3).

1.4.4.14.5. **(Added-AFMC)** Coordinate with the installation ATO to publish AT articles in available media, which reaches and educates the base populace on AT efforts and information.

1.4.4.15. Command Post Mangers shall:

1.4.4.15.1. Conduct operational reporting IAW AFI 10-206, *Operational Reporting (T-1)*.

1.4.4.15.2. Establish procedures for information dissemination from GCCs to AF components (i.e., FPCON changes, travel restrictions, advisories, etc.) (T-0).

1.4.4.15.3. **(Added-AFMC)** Ensure installation ATO is notified on information/events that meet CCIR, PIR, SIR, and SAR requirements, when applicable.

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, insider threat plans, emergency management plans, Disease Containment Plan (DCP), 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 all appropriate agencies to ensure that AT program requirements and considerations are factored into planning for programs under their control and authority.

1.4.5.3. **(Added-AFMC)** The ATO will ensure coordination with CE, FSS, MDG, and CARM Manager for consolidating and conducting of local assessments at the same time as the LVA. (T-2)

1.4.6. Unit AT Representatives (ATRs). 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 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) **(T-0)**. 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 US 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 rules are followed **(T-0)**. 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 **(T-2)**.

2.2.2.3. Identify an AFOSI official as the focal point for local or host nation law enforcement intelligence, CI and criminal information **(T-2)**.

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 **(T-3)**. (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 **(T-3)**.

2.2.2.5. Establish guidance, program, allocate resources, 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 and A4). Ensure units in-transit are provided with tailored terrorist threat information (**T-2**).

2.2.2.6. (**AFMC**) Include counter-surveillance/surveillance detection protocols in the AT Plan or reference to appropriate plan. Refer to the Joint Antiterrorism (JAT) Program Managers Guide and Tools for template and additional considerations.

2.2.2.7. Establish procedures to rapidly receive, evaluate, analyze and disseminate all relevant threat data with AFOSI, Security Forces and other staff force protection elements. Ensure procedures are established to track Intelligence Community 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, High-Risk Personnel, 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.

2.2.2.9. Ensure intelligence for the AT program is provided by organic Intelligence elements IAW AFI 14-119 and all relevant guidance and doctrine (**T-0**).

2.2.3. Air Force intelligence, CI and law enforcement elements will coordinate the dissemination of information on US persons as appropriate in support of the AT Program and within the provisions of AFD 71-1, AFI 71-101 Volume 1, *Criminal Investigations Program*, and AFI 71-101 Volume 4, *Counterintelligence* (**T-0**). The collection, use, retention and dissemination of intelligence or other information relating to US persons is highly regulated. AFOSI, intelligence units and other organizations involved in Air Force antiterrorism efforts must conduct training on, and comply with, restrictions on conducting intelligence activities on US persons as contained in DoD 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*, AFI 14-104, *Oversight of Intelligence Activities*, and Executive Order 12333, *United States 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

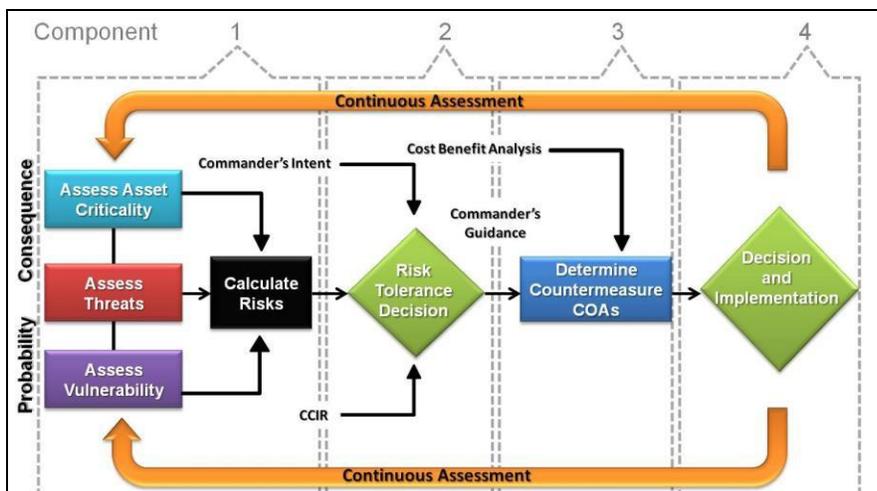
facilities, programs and systems to an attack, including the use of CBRN (including TIC/TIM), explosive hazard (EH) or similar capabilities (vulnerability assessment); assessing risk based on a holistic understanding of the criticality, threat and vulnerability of the asset (risk assessment); and implementing 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 annually, or as changes occur (T-1).

2.3.1. (AFMC) Installations will ensure coordination and integrate of all other AF risk management associated programs to the fullest extent possible [e.g., Critical Asset Risk Management (CARM), Continuity of Operations (COOP), and Emergency Management (EM)]. (T-2)

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 (T-0). See Figure 2.1 for a graphic depiction.

Figure 2.1. AT Risk



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 CBRN) (T-0). 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 (T-0). 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 (T-0). AFOSI is the AF agency responsible for preparing the LTA as prescribed in DoDI 5240.18, *Counterintelligence (CI) Analysis and Production* 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 (T-1). The DBT will be used to help establish the base's defensive posture and is critical for engineering projects and renovations (T-1). 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 (T-0).

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 US 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 force health protection 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 (T-0).

2.5. Standard 5: Criticality Assessment.

2.5.1. Criticality assessment processes shall be conducted in accordance with 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 (T-0).

2.5.1.2. Criticality assessments shall be updated at least annually to determine the degree of asset criticality (T-0). 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., installation AT Plan, Installation Emergency Management Plan (IEMP) 10-2, Contingency Response Plan (CRP), MCRP, IDP, etc.).

2.5.2. Criticality assessments should be coordinated with DCIP and Air Force CARM program managers. 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.

2.5.3. **(Added-AFMC)** A Critical Asset List (CAL) will be built from the ForcePRO Criticality Assessment and will be utilized by the installation to develop all other priority list (e.g., response priority list, fire response priority list, generator support list, infrastructure support list, etc.).

2.6. Standard 6: Terrorism Vulnerability Assessment. VA processes will be conducted per DoDI 2000.16. 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], CBRN and DCIP assessments) to reduce the impact on operational units.

2.6.1. DoD and COCOM benchmarks will be used to guide all VAs **(T-0)**. 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 **(T-1)**.

2.6.2. A VA will be conducted at least annually or as threat or mission requirements dictate **(T-0)**. Installation ATOs shall report completion of their local VA to their higher headquarters **(T-0)**. Completed VA reports shall be entered into CVAMP and reviewed by the MAJCOM **(T-0)**. VAs shall be conducted at a minimum for, but not limited to:

2.6.2. **(AFMC)** AFMC Installation ATOs will forward a schedule of forecasted LMA/LVAs to the AFMC ATPM by 15 January of each CY. **(T-2)**

2.6.2.1. Any AF installation or AF-owned or leased facility populated daily by 300 or more DoD personnel **(T-0)**.

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 program; or any AF research facility registered by the United States Department of Health and Human Services (HHS)/Centers for Disease Control and Prevention (CDC), and/or the United States Department of Agriculture (USDA)/Animal and Plant Health Inspection Service (APHIS) to use, possess, transfer, or receive biological select agents and toxins (refer to DoDI 5210.89_AFI 10-3901, *Minimum Security Standards for Safeguarding Biological Select Agents and Toxins*) **(T-0)**.

2.6.2.3. Any AF installation, facility, or activity involving interaction with local non-military or host nation agencies **(T-0)**.

2.6.2.4. AF-hosted air ports of embarkation and debarkation; 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 **(T-0)**. AF movement or shipment

of military cargo shall be coordinated with the designated senior DoD Component with AT responsibility **(T-0)**.

2.6.2.5. Any AF personnel designated as HRP (Standard 16). These assessments are referred to as Personal Security Vulnerability Assessments (PSVAs) **(T-0)**. 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 **(T-0)**.

2.6.2.6. Any AF event or activity determined to be a special event involving a gathering of 300 or more DoD personnel **(T-0)**. Consider creating a Special Events Assessment Plan or template tailored for such activities.

2.6.2.6.1. **(Added-AFMC)** Installations will identify, in their AT Plan, the size of the special event which the TWG will be required to coordinate on, as well as the minimum requirements special event coordinators will be mandated to fulfill prior to and during the event to ensure the safety and security of personnel. **(T-2)**

2.6.2.7. AF-owned or leased off-installation facilities, privatized housing, off-base community 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 **(T-0)**. 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 **(T-0)**.

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 AFMAN 10-246 for Food and Water VA requirements) **(T-0)**.

2.6.4. Information derived from VAs shall be classified pursuant to the requirements outlined in the Defense Threat Reduction Agency's (DTRA) Security Classification Guide for Vulnerability Assessments **(T-0)**. Information related to DCIP assets shall be classified pursuant to the requirements outlined in the DCIP Security Classification Manual (DoDM 3020.40 Volume III) **(T-0)**.

2.6.5. AT vulnerability assessments conducted by the local installation, the AF VA Team (AF VAT), or any other HHQ level, shall include a review of any vulnerability or concern identified in previous VAs (from any source/level) which remains open (i.e., not—accepted or mitigated) **(T-2)**.

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 **(T-0)**. 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 **(T-2)**.

2.6.6.1. **(Added-AFMC)** If appropriate, include estimated cost of reducing vulnerability/area of concern in CVAMP commander comments and ACES number.

2.6.6.2. **(Added-AFMC)** When IDRMP is used, ensure that CVAMP and ForcePRO recommended courses of action are synchronized. The installation ATO will also assure that all documentation of risk acceptance is consistent between CVAMP and IDRMP. (T-2)

2.6.6.3. **(Added-AFMC)** Installation shall address procedural and low-cost AT vulnerabilities identified during all vulnerability assessments.

2.6.6.4. **(Added-AFMC)** Critical and high risk vulnerabilities/risk must be addressed by funding or improved security tactics, techniques and procedures and risk must be reassessed until it is at a lower acceptable level or risk was assessed and accepted by the decision-maker (commander or civilian equivalent director) in writing and placed into CVAMP. See the *DoD Antiterrorism Officer Guide* for discussion on strategies to mitigate major/high risk vulnerabilities.

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 **(T-3)**). 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 **(T-3)**. 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 monthly **(T-3)**. The installation ATWG and ATEC will semi-annually review open CVAMP vulnerabilities and concerns **(T-2)**.

2.6.7.2.1. **(Added-AFMC)** Ensure review is documented in ATWG and ATEC meeting minutes.

2.6.7.3. Installation Commanders may authorize installation ATO's "Commander's Privileges" within CVAMP to aid in database maintenance. Such authorization will be in writing, and may be included on the ATO appointment letter **(T-3)**. However, this does not relieve the commander from having situational awareness of the data within CVAMP.

2.6.7.3.1. **(Added-AFMC)** Installation ATO Appointment and CVAMP Administrator(s) Letters (as required in para 2.6.7.3.) will be combined (T-3). ATOs that are given "Commanders Privileges" are not afford the authority to make commander decisions without the commander's knowledge and/or approval; nor does this delegation relieve the commander from having situational awareness of the data.

2.6.7.3.2. **(Added-AFMC)** Installation Commander shall review all open concerns and vulnerabilities within 60 days of assuming command.

2.6.7.3.3. **(Added-AFMC)** Installation Commander shall conduct a review of all observations (vulnerabilities and concerns), concur or non-concur with the ATWG's recommendations, and add a mitigation plan and release observations to the next level.

2.6.7.4. **(Added-AFMC)** Installation ATOs shall report CVAMP Vulnerability/Concern/UFR status and command observation trend analysis on a semi-annual basis to Center leadership.

2.6.7.5. **(Added-AFMC)** Ensure cost estimates for fixing CVAMP vulnerabilities/concern are located on the last line in the “discussion field.” This will allow the data to be collected by AF/A4S for programming funds.

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 USAFSAM, appropriate MAJCOM IG Gatekeepers and ATPMs to complete any HHQ VA not covered by DTRA or COCOM teams. The AF VAT will also work with the appropriate MAJCOM IG Gatekeepers and ATPMs to ensure maximum availability of subject matter experts if the AFVA is conducted in conjunction with on-site periodic or capstone 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 risk management requirements. Where possible, AF CARM assessments 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 commander through the owning MAJCOM IG to the Commander, 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.

2.6.8.2. **(AFMC)** Installations who submitted a request for HHQ VA cancellations or schedule changes will courtesy copy AFMC ATPM. (T-2)

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 AF VAT.

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. 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 semi-annually review installation CVAMP entries.

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, cyberspace operations specialist and EOD specialist, when appropriate. Other functional experts may augment the team as needed, such as Information Protection, depending on the type of assessment required (comprehensive or targeted), the nature of the installation's mission, and the terrorist threat level.

2.6.11.1. **(Added-AFMC)** AFMC and subordinates will use the most current guidelines and criteria stipulated in the DoD Mission Assurance Benchmarks to standardize the MA/VA process for coherency throughout the command (T-2).

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 **(T-0)**. Installation AT plans must be cross-referenced, compatible, and synchronized with other base plans (IDP, IEMP 10-2, MCRP, etc.) **(T-1)**. To optimize protection planning efforts, the installation AT plan can be combined with other installation plans in an integrated plan structure to fully capture and coordinate response capabilities. 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 **(T-0)**.

2.7.1. **(AFMC)** It is highly recommended that installations utilize the Joint Antiterrorism (JAT) Guide to develop their AT Plans as the JAT Guide format will ensure all DoD and AF required areas of the AT Plan are met. Installations can eliminate areas in the JAT Guide template as needed. Separate AT Plans are only required if facilities, deployments, training exercise deployments, and special events procedures/actions are not already included into the installation's AT Plan.

2.7.1.1. Installation AT plans will specify requirements for unit AT plans and programs **(T-2)**. 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 standalone plan **(T-0)**. However, they will develop an AT plan or instruction for their unit detailing procedures for integrating into the host installation's AT plan **(T-2)**. ANG and AFR tenant units will appoint an ATR for each unit and will participate fully in the host installation's AT program **(T-0)**.

2.7.1.2. Installation commanders will review and sign AT plans within 60 days of taking command (**T-2**).

2.7.1.2. (**AFMC**) AT Plan will be reviewed annually or when the mission or threat changes. Installation commanders shall document a review of the Installation AT Plan on an annual basis. Installation ATOs must maintain the commander's review with the AT Plan.

2.7.1.3. (**Added-AFMC**) A copy of the installation AT Plan will be placed on AFMC's EIM site within 30 days of being signed by the Installation Commander.

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 AF/A4C (CE) is designated the OPR, refer to AFI 10-2501.

Table 2.1. AT Threat Planning Scenarios

NOTE: Scenarios are numbered to correspond to the national scenarios, except for AF added scenarios.		
Scenario	Title	OPR
1	Nuclear Detonation – 10-Kiloton Improvised Nuclear Device	A4C (CE)
2	Biological Attack – Aerosol Anthrax	SG3/5 (Medical)
4	Biological Attack – Plague	SG3/5 (Medical)
5	Chemical Attack – Blister Agent	A4C (CE))
6	Chemical Attack – Toxic Industrial Chemicals	A4C (CE)
7	Chemical Attack – Nerve Agent	A4C (CE)
8	Chemical Attack – Chlorine Tank Explosion	A4C (CE)
11	Radiological Attack – Radiological Dispersal Devices	A4C (CE)
12	Explosive Attack – Bombing Using Improvised Explosive Devices	A4C (CE)
13	Biological Attack – Food Contamination	SG3/5 (Medical)
15	Cyberspace Attack	SAF/CIO A6 or AF/A3C
16 (AF)	Armed Attack – Small Arms: Individual to 10 persons (includes active shooter)	A4S (SF)
17 (AF)	Attacks on Aircraft in the Take-off and Landing Footprint	A4S (SF)
18 (AF)	Stand-off Indirect Fire	A4S (SF)
19 (AF)	Sniper Attack	A4S (SF)
20 (AF)	Hostage Crisis	A4S (SF)
21 (AF)	Contamination of Drinking Water System	SG3/5 (Medical)
22 (AF)	Extended Loss of Energy Supply	A4C (CE)

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. (AFMC) When AT actions (e.g., barrier plans, risk mitigation measures, incident response, etc.) required by AT Plans are contained in other plans, the overall AT Plan is not complete unless all referenced plans are executable.

2.7.3.1. The minimum essential AT program elements (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 **(T-0)**.

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 installation AT plan **(T-0)**.

2.7.3.4. AT risk mitigation measures for AF off-installation facilities, housing and activities (Standard 15) **(T-0)**.

2.7.3.5. AT risk mitigation measures for HRP (Standard 16) **(T-0)**.

2.7.3.6. AT construction and building considerations (Standard 17) **(T-0)**.

2.7.3.6.1. **(Added-AFMC)** Installation AT Construction review procedures will be included in the AT Plan.

2.7.3.7. AT risk mitigation measures for logistics and other contracting (Standard 18) **(T-0)**.

2.7.3.8. AT risk mitigation measures for critical asset security (Standard 19) **(T-0)**.

2.7.3.9. AT risk mitigation measures for in-transit movements **(T-0)**.

2.7.3.10. AT incident response measures (Standard 20) **(T-0)**.

2.7.3.11. Terrorism consequence management measures, including CBRN mitigation planning (Standard 21 and IEMP 10-2) **(T-0)**.

2.7.3.12. FPCON implementation measures, including site-specific AT measures (Standard 22) **(T-0)**.

2.7.3.12. **(AFMC)** FPCON implementation must include processes for setting FPCON levels, FPCON transition (both up and down), FPCON dissemination to both facilities and personnel located on and off the installation, and FPCON waiver process.

2.7.3.13. **(Added-AFMC)** Curtailment Plan. Address curtailment measures as FPCONs increase. Examples of curtailed functions include, but not limited to: non DOD/Air Force affiliated civilian access to the base for military-sponsored events (e.g., weddings, holiday parties, etc.); sports events; bazaars; professional meetings; access to AAFES facilities, college student registration/access and pass control, etc. Actions must be referenced in FPCON Checklist.

2.7.3.14. **(Added-AFMC)** MANPAD Mitigation Plan.

2.7.3.15. **(Added-AFMC)** Surveillance Detection (SD) and Countersurveillance (CS) Plan.

2.7.3.16. **(Added-AFMC)** Special Event VA Procedures.

2.7.3.17. **(Added-AFMC)** CCIRs and PIRs.

2.7.4. AT planning information for deploying DoD units may be provided by GCCs (e.g., airfield, port, and movement route information and criticality, threat, and VA data). 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 first and emergency responders (civilian and military) onto the installation during emergencies under all FPCONs (T-0).

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 (T-0).

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 (T-2).

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 (T-0). 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 perform temporary duty, commanders will immediately contact the AFOSI unit or ATO responsible for that AOR (T-2). 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 (T-0). Where support agreements such as MOUs, MOAs or MAAs 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) (T-0).

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 (T-0). 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 (T-0). 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 (T-0).

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. 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) (T-3). 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. (AFMC) The ATO appointment letter will list the DFC/CSF as the installation ATO and the person(s) executing the duties and responsibilities for the DFC/CSF as the alternate ATO. All AFMC installations/sites/plants will submit a copy of the appointment letter on AFMC AT EIM site within 30 days of appointment (See Atch 9 for required format). All appointed installation ATOs within AFMC will be trained by a formal USAF Level II AT course as soon as possible of appointment. Wings will have ATOs appointed to support their unit ATRs. Appointment letters will list a primary and alternate (See Atch 10 for required format). **NOTE:** If unable to meet rank/grade or military/civilian requirement(s) as defined in paras 2.9.1., 2.9.1.1. or 2.9.1.3., a waiver IAW AFI 33-360 must be completed.

2.9.1.1. Installation and separate facility (those not supported by a host installation AT program) or higher levels (T-0). At the installation, the SF Group Commander or SF Squadron Commander will be dual-hatted as the installation ATO to provide Wing Commanders with a single focal point for all installation AT and physical security matters (T-1). The support staff for the ATO duties will reside in the SFG staff or SFS S-5 staff (T-1).

2.9.1.2. Deploying units having 300 or more personnel assigned will have a Level II-certified ATO (T-0).

2.9.1.3. All other units not qualifying for an ATO as outlined in paragraphs 2.9.1.1 and 2.9.1.2. will have a unit ATR appointed in writing by the unit commander or element chief **(T-1)**. 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 **(T-3)**. ATR training is outlined in Standard 26.

2.9.1.3. **(AFMC)** If an organization is unable to meet the rank requirement of this paragraph (E-5/GS-5) a waiver IAW AFI 33-360 must be completed **(T-2)**. Ensure Installation Commander's staffing requirements are listed in the installation's AT Plan. Appointment letters will list a primary and alternate.

2.9.2. All ATOs 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 **(T-3)**.

2.9.2.2. Recommend guidance, priorities and resourcing strategies for the correction or mitigation of AT vulnerabilities to the ATEC **(T-2)**.

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 **(T-2)**.

2.9.2.4. Provide AT considerations, to include real-world and exercise lessons learned, to assist the installation/facility inspection team in developing realistic and relevant scenarios to exercise and validate the AT program **(T-2)**.

2.9.2.4. **(AFMC)** Installation ATO or designated representative will be a part of the Wing Inspection Team (WIT) and approve all AT related scenarios/exercises to ensure relevance and intent.

2.9.2.5. Collaborate with the TWG to determine if action through warnings, policy and 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 and guidance, or organize, train and equip functions are necessary based on worldwide terrorism incidents or threats **(T-1)**.

2.9.2.6. Work closely with AFOSI to support and advocate the Air Force Eagle Eyes program **(T-3)**.

2.9.2.7. Participate in installation working groups, such as the IDWG, ATWG, TWG, EMWG, CARM WG, Insider Threat working group, Facilities Board, and Medical working groups, as necessary **(T-2)**.

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

2.9.3.1. In order to effectively coordinate on threat data with AFOSI and Force Protection Intelligence (FPI) representatives, the installation ATO requires appropriate

clearance and access to Top Secret (TS) Sensitive Compartmented Information (SCI) with Signal Intelligence/Talent Keyhole (SI/TK), Human Intelligence Control System (HCS) and Gamma (G) SCI caveats **(T-2)**. 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.

2.9.3.1. **(AFMC)** Person appointed to execute the duties and responsibilities of the installation ATO will have the same clearance requirements listed in this paragraph.

2.9.3.1.1. **(Added-AFMC)** All AFMC installations shall ensure installation ATOs have immediate SIPRNET access.

2.9.3.2. Ensure CVAMP is populated with all observations from assessments and program review reports IAW this instruction **(T-0)**. 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 **(T-0)**.

2.9.3.3. 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 **(T-0)**. Where emergency or newly-emergent requirements occur, recommend and document requests/concerns for CCIF funding IAW para 2.9.2.3. of this publication.

2.9.3.4. AF CARM critical asset data and assessments will be populated and tracked by the CARM manager in AF-CAMS **(T-0)**.

2.9.3.5. Monitor and manage funds provided in PEC 28047F and coordinate funding for AT vulnerabilities identified in CVAMP and other AT initiatives **(T-2)**.

2.9.3.6. Assist the DFC's staff in facilitating AT issues before the ATWG and ATEC, or other related working groups and councils as appropriate **(T-3)**.

2.9.3.7. Coordinate with intel and AFOSI representatives to ensure the commander's CCIRs and PIRs are developed **(T-3)**.

2.9.3.8. Assist the Civil Engineer Squadron in the development of DBTs **(T-2)**.

2.9.3.9. Coordinate for local and HHQ VAs **(T-3)**.

2.9.3.9.1. **(Added-AFMC)** Coordinate with installation agencies (CBRNE, Food/Water, CARM, etc.) to align as many assessments together to reduce the impact on the installation. The Installation ATO will be the team chief for the local combined assessment.

2.9.3.10. Coordinate multifunctional teams of subject matter experts (SMEs) when conducting required AT assessments (vulnerability, criticality, and threat assessments) **(T-2)**. Provide results of each assessment to the designated Security Forces POC for inclusion in the IDRMP **(T-3)**.

2.9.3.11. 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.

2.9.3.12. Direct the installation RAM program in close coordination with executing units **(T-3)**.

2.9.3.12.1. **(Added-AFMC)** Accomplish spot-checks on unit conducted RAMs to ensure units are accomplishing them IAW installation's established guidelines. Document spot-checks IAW locally establish procedures.

2.9.3.13. Provide ATRs with electronic and/or hardcopy materials for use in unit continuity binders **(T-3)**. 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.

2.9.3.14. **(Added-AFMC)** Use attachment 8 to conduct Unit Program Reviews (UPRs) no less than every 18 months on all units and tenants located on the installation.

2.9.3.15. **(Added-AFMC)** Attended meeting and working groups as required by installation ATO.

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 **(T-3)**.

2.9.4.1.1. **(Added-AFMC)** Develop site-specific FPCON measures for the unit/facilities and ensure they are reviewed by Installation ATO and approved by the unit commander/civilian equivalent.

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 **(T-3)**.

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 **(T-3)**.

2.9.4.5. Assist the installation ATO with AT program implementation, where applicable **(T-3)**.

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 **(T-2)**. Encourage the same for dependent family members.

2.9.4.7. **(Added-AFMC)** Ensure all unit personnel are aware of the Installation Commander's Travel Policy for travel outside the CONUS.

2.9.4.8. **(Added-AFMC)** Ensure assigned personnel are aware of the requirement for AT Travel Plans for all DOD personnel traveling or deploying to countries outside the USNORTHCOM AOR that are not a part of the US, its territories, or possessions. DOD civilians, contractors and family members must abide by USNORTHCOM AT policies

and procedures when working and/or traveling in an official capacity. Unit ATRs are responsible for completing the AT Travel plans IAW NCI 10-222 Chapter 24.

2.9.4.9. **(Added-AFMC)** Personnel deploying outside of the USNORTHCOM AOR into another Combatant Commander's AOR must follow the specific AT guidelines set forth by that Combatant Commander.

2.9.4.10. **(Added-AFMC)** Develop unit antiterrorism instructions for personnel and areas under their control. At a minimum, the instruction will include unit ATR duties and responsibilities, procedures for bomb threats, active shooters, suspicious mail and mail handling procedures, suspicious packages, parking plan (moving container and vehicles away from the facility(s) IAW UFC 4-010-01), and building evacuations. Ensure instruction is reviewed annually or when changes occurred by unit commander or civilian equivalent.

2.9.4.11. **(Added-AFMC)** Develop instructions on door-guard responsibilities and ensure personnel are trained on responsibilities for holding these duties during RAMs and higher FPCONS.

2.9.4.12. **(Added-AFMC)** Participate, or ensure appropriate SME participation in the annual Risk Assessment process, when required/requested.

2.9.4.13. **(Added-AFMC)** Attended meeting and working groups as required by installation ATO.

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 **(T-0)**. ATWGs oversee the implementation of the AT program, develop and refine AT plans; 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. **(AFMC)** ATWG duties and responsibilities will also include the following: installation site-specific FPCON measures, validation of the installation Critical Asset List (CAL), ATWG Charter review, and development of site-specific contractor risk mitigation measures (e.g., inspections, spot-checks, patrols, suspicious activity reporting, FPCON briefing, Giant Voice, no-go areas, AT Level I training, circulation control, etc.) for inclusion into contracts and FPCONS measures, and assessment mitigation plan as defined in para 2.6.6. in parent AFI.

2.10.2. The chairperson and members of the ATWG will be designated in the installation AT Plan **(T-3)**. The ATWG is usually composed of the ATO, CARM Manager, Information Protection, 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.

2.10.2.1. To optimize force protection capabilities, installations may combine the ATWG, IDWG and EMWG into a single working group. Consider combining/including other related working groups as appropriate. Installations may also establish a “planning” sub-working group to a combined working group, which focuses on maximizing efficiencies, reviewing and refining installation plans such as the IDP, IEMP 10-2 and AT Plan. Co-locating these planning functions may also produce additional benefits. If combined, ensure working group minutes clearly identify AT-related agenda items so that a record is maintained of AT-related decisions, discussions and activities.

2.10.2.1.1. **(Added-AFMC)** ATWG member’s security clearance requirements will be codified in the ATWG Charter or AT Plan. If the ATWG Charter is located outside of the AT Plan, the Charter must be signed by the Installation Commander. If combined with other working groups a combined Charter can be developed and placed in one plan. Charter will be reviewed annually and documented in the meeting minutes. ATWG will be chaired by an O-6/Group CC or civilian equivalent to ensure the proper emphasis is placed on the importance of this working group.

2.10.2.2. Maintain a minimum of the last 12 months of meeting minutes on file **(T-3)**. Units will ensure they follow table and rule guidelines located in the AF Records Disposition Schedule (RDS) and maintain this reference data for unit continuity and action as required.

2.10.2.2. **(AFMC)** ATWG meeting minutes shall be signed by the chairperson and maintained for 24 months.

2.10.3. At the HAF level, the ATWG is combined with the SE/MA Working Group. AF/A4SO and SAF/AAZE co-chair the HAF SE/MA Working Group. The HAF SE/MA Working Group is an action officer-level group, meeting semi-annually or more frequently as needed, to coordinate and integrate Security Enterprise, Mission Assurance and Antiterrorism efforts as directed by the HAF SE/MA Steering Group. 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 **(T-0)**. The TWG is required to meet at least quarterly or more frequently, depending upon the threat activity **(T-0)**. The TWG should be activated at least semiannually in response to installation-level antiterrorism exercises. TWGs develop and refine terrorism threat assessments and coordinate and disseminate threat warnings, reports, and summaries.

2.11.1.1. **(Added-AFMC)** In addition to the duties and responsibilities listed above, the TWG will assist in the development of the Commander’s Critical Information Requirements (CCIRs), Priority Intelligence Requirements (PIRs), the Design Basis Threat (DBT)

2.11.2. The TWG will be chaired by the installation commander (or designated representative) and is composed of the ATO, Intelligence, AFOSI, Security Forces, Public Affairs, and Legal **(T-2)**. Additional membership, such as Information Protection, can be added based on the threat. Security clearance requirements for members will be established by the commander.

2.11.2.1. **(Added-AFMC)** When delegated, the chair of the TWG will be no lower than the installation's Vice-Commander or equivalent. (T-2)

2.11.2.2. **(Added-AFMC)** When necessary and as directed by installation leaders, invite host nation or civilian law enforcement as well as joint and/or combined forces representatives to attend the installation TWG.

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

2.11.4. The TWG may be leveraged to support the Air Force Insider Threat Program IAW AFI 16-1402, *Insider Threat Program Management*.

2.11.5. **(Added-AFMC)** All TWG meeting minutes shall be signed by the chairperson and maintained for at least 24 months.

2.11.6. **(Added-AFMC)** All TWG members shall review the TWG Charter for accuracy and updates at least annually.

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 semiannually or as directed by the commander (i.e., emerging threats or the accomplish the IDRMP) **(T-0)**. 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 designated representative) and is composed of group commanders (or designated representatives). The chair and members of the ATEC will be designated in the installation AT Plan **(T-2)**. The ATEC is supported by the ATO, Intelligence, AFOSI, Security Forces, Communications, Information Protection, Emergency Management, Critical Asset Risk Management, EOD, Logistics Readiness, Medical Readiness, Public Affairs, Legal, Airfield Operations, Financial Management, major tenants, and supported Components on a Joint Base consistent with parent Service directives and local MOUs **(T-2)**.

2.12.2. **(AFMC)** Minimum membership will include tenant wing commanders and tenant group commanders if not represented by a wing commander. Chairperson will be designated no lower than the Installation Vice Commander.

2.12.2.1. **(Added-AFMC)** ATEC member's security clearance requirements will be codified in the ATEC Charter or AT Plan. If the ATEC Charter is located outside of the AT Plan, the Charter must be signed by the Installation Commander. Charter will be reviewed annually and documented in the meeting minutes.

2.12.3. On AF installations and self-supported separate facilities, the ATEC should be combined with the IDC. If combined, ensure meeting minutes clearly identify AT-related agenda items so that a record is maintained of AT-related decisions, discussions and activities. Maintain at least the past 12 months of meeting minutes on file **(T-3)**. Coordinate with other executive groups to eliminate redundant records and efforts. Units will ensure they follow table and rule guidelines located in the AF Records Disposition Schedule (RDS). The ATEC will conduct a semiannual review of all AT deviations, local FPCON measures,

installation risk assessments, open CVAMP observations, installation AT plan, and RAM execution (T-2).

2.12.3.1. (Added-AFMC) ATEC meeting minutes shall be signed by the chairperson and maintained for 24 months.

2.12.4. At the HAF level, the ATEC shall be constituted within the HAF SE/MA Steering Group. AF/A4S and SAF/AAZ co-chair the HAF SE/MA Steering Group. The HAF SE/MA Steering Group 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 Security Enterprise, Mission Assurance and Antiterrorism efforts. The SE/MA Steering Group supports the Air Force Security Enterprise Executive Board (AFSEEB). IAW AFD 16-14, the AFSEEB is the senior-level governance body for the strategic oversight, administration, policy synchronization, resource review and prioritization, and risk management activities of the Air Force Security Enterprise. 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 and DoD 5200.08-R, *Physical Security Program*, 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, perimeter and area security, access and egress control, protection against CBRN attacks (including those using the postal system and food/water supplies), explosive hazard protection, 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 (T-0).

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 (T-2).

2.13.3.1. The Navy is 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>.

2.13.4. Ensure installation access control points and associated barrier plans are constructed and operated IAW 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* (T-0).

2.13.4.1. Installations will enforce proper standoff following UFC 4-010-01. 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.

2.13.4.3. **(Added-AFMC)** Barrier plans will be detailed to protect critical facilities from vehicle attacks. The barrier plan for the critical facility/asset must be developed/created from the criticality asset list approved by the Installation Commander. Ensure DBT is utilized for development/updating of the barrier plan.

2.13.4.4. **(Added-AFMC)** Barrier plans must include countermobility at the perimeter. Countermobility can include natural or manmade barriers (e.g., ditches, heavily wood areas, concrete barriers, cabling, etc.) and all permanently fixed barriers (e.g., final denial barriers, vehicle containment, bollards, etc.).

2.13.5. **(Added-AFMC)** If AT Physical Security Measures are not listed in the AT Plan, it must be referenced.

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

2.14.1. The RAM program is developed and implemented as an integral component of the overall AT program. 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 **(T-0)**. Random use of other security measures, to include technologies, should be used to supplement FPCON measures. The RAM program shall be included in installation AT plans **(T-0)**.

2.14.1.1. **(Added-AFMC)** Off-installation facilities with 300+ personnel assigned will conduct at least (1) daily RAM, off-installation facilities with 299 to 50 personnel will conduct at least 3 RAMs weekly (when occupied) and off-installation facilities with 49 to 11 personnel will conduct at least 1 RAM weekly (when occupied). Off-installation facilities are not afforded the same security opportunities as the installation and could be viewed as a less protected area and vulnerable to attack.

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

2.14.2.1. Include tenant units and organizations **(T-0)**.

2.14.2.2. Implement daily RAMs to include weekends and holidays. The frequency will be increased as the threat increases **(T-2)**. At least three RAMs chosen from higher FPCONs are required daily **(T-2)**.

2.14.2.2.1. **(Added-AFMC)** RAMs conducted by posted Security Forces personnel will not count towards the installation's daily required RAMs.

2.14.2.2.2. **(Added-AFMC)** The minimum number of RAMs required for each FPCON will be (3) Normal/Alpha, (4) Bravo and (5) Charlie.

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

2.14.2.3. (AFMC) RAMs will be developed to lower unacceptable risks to within the commander's identified risk acceptance level or at a minimum reduce risk.

2.14.2.4. RAM implementation shall be compatible and coordinated with ongoing law enforcement or CI surveillance detection and ID measures (T-2). When random vehicle inspections are employed as a RAM, pre-coordinate with the installation legal office (T-2). Follow existing law enforcement rules when employing random vehicle inspections as a RAM.

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

2.14.2.6. Include local, state, federal, and host nation law enforcement patrols and first responders, as appropriate (T-3).

2.14.2.7. Implement RAMs installation-wide or focused on facilities or functions identified as potential targets (T-3). When implementing facility-specific RAMs, consider the possibility that 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 (T-3). Effectiveness of RAMs should be measured by the ATO and analyzed by the TWG.

2.14.2.8. (AFMC) RAM tracking documentation will be maintained for a minimum of 1 year.

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

2.15.1. Installations shall include specific AT measures for AF-owned or leased off-installation facilities, privatized housing, off-base community 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 (T-0). At locations where there are multiple DoD components or locations, AT measures shall be coordinated with the designated senior DoD Component with AT responsibility (T-0).

2.15.1.1. (Added-AFMC) For every DoD-owned, leased, or managed off-installation facility, appoint either a Designated Official (DO) or Senior Official (SO), who shall have FP responsibility IAW NCI 10-222.

2.15.1.2. (Added-AFMC) For DoD and non-DoD-owned, leased, or managed facilities occupied by DoD personnel, the DO/SO will ensure all appropriate Air Force, MAJCOM and site-specific FPCON Measures are implemented in the DoD-occupied portions of the building.

2.15.2. Risk mitigation measures for AF-owned or leased off-installation facilities, privatized housing, off-base community 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, CBRN and explosive hazard defensive measures and shelter-in-place (ensure

consistency and interoperability with IEMP 10-2), and relocation and evacuation procedures **(T-0)**.

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 **(T-0)**.

2.15.3.1. Ensure such agreements are reviewed annually by the OPR, ATWG and JA for currency and executability **(T-2)**. 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 OPR for support agreements **(T-2)**.

2.15.4. **(Added-AFMC)** Coordination with installation ATO is required prior to signing a lease agreement for facilities.

2.15.5. **(Added-AFMC)** Installations will ensure compliance with Physical Security Criteria for Federal Facilities for all new and renewing leases.

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

2.16.1. Develop AT measures pursuant to the principles outlined in DoDI O-2000.22, and AFI 71-101, Volume 2, *Protective Service Matters*, for personnel designated as HRP **(T-0)**.

2.16.1.1. SAF/IGX is the HAF focal point for policy development and coordination with the Office of the Assistant Secretary of Defense 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 (PSDs) 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 SecAF, USecAF, CSAF, and VCSAF 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 a 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 **(T-0)**. PSVAs will be revalidated annually and updated if the TTL changes, but no less than every 3 years **(T-0)**.

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); be properly cleared for assignment to positions, facilities or countries requiring such protection; and be thoroughly indoctrinated on the duties and responsibilities of protective service personnel **(T-0)**.

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 **(T-0)**.

2.16.6. HRP security measures shall be reviewed within 60 days of changes to the TTL for the affected country and HRP **(T-0)**.

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 **(T-1)**.

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.

2.17.1.1. **(Added-AFMC)** The Base Civil Engineer, in coordination with the installation ATO will prepare a deviation request IAW Attachment 6 where the DoD Minimum Antiterrorism Standards for Buildings cannot be met for new construction or major renovation projects that require compliance.

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 comply with UFC AT standards **(T-0)**.

2.17.4. Engineering staff will work with the ATO from design inception to project completion, to ensure AT requirements are met **(T-2)**. The ATO shall be part of the coordination process prior to certification **(T-2)**.

2.17.5. Ensure CE and the ATO develop a prioritized list of risk mitigation measures (reference UFCs and AFI 31-101) for use by site selection teams. **(T-0)** 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. **(T-0)** Circumstances may require the movement of DoD personnel or assets to facilities the US

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 A4C (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 US 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 **(T-0)**. 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.

2.18.1.1. **(Added-AFMC)** AFMC Contracting Directorates (PK) or Installation Contracting, in coordination with the Installation ATO and Security Forces will ensure basic security and AT language is developed for inclusion in all performance work statements (PWS), contract data requirements lists (CDRL) or other requirements documents (e.g., inspections, spot-checks, patrols, suspicious activity reporting, FPCON briefing, Giant Voice, no-go areas, AT Level I training, circulation control, etc.). Document the process IAW NCI 10-222 and include in the AT Plan.

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 **(T-0)**. 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 in accordance with the established SOFA **(T-0)**.

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 **(T-0)**.

2.18.3.1. **(Added-AFMC)** Security measures, at a minimum, shall address elements such as contractor screening, access control, favorable fingerprint or NCIC results, circulation control special security concerns, and training. NOTE: See AFMC Added 2.18.1.1. for further suggestions.

2.18.3.2. **(Added-AFMC)** Include site-specific contracting risk mitigation measures in locally developed FPCONs Measures Checklist.

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 **(T-0)**.

2.18.5. Contracts shall comply with the AT clauses of the DFARS (T-0).

2.18.6. Contracts shall incorporate Level I – AT Awareness Training requirements (Standard 25) (T-0).

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 (T-0). 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 (T-0).

2.19.3. Criticality assessments conducted on critical assets identified as part of the DCIP and Air Force CARM programs will be conducted IAW DoDD 3020.40 and AFPD 10-24 (T-0).

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 installation AT plan (T-0). These measures shall include procedures for determining the nature and scope of incident response (including incidents with a CBRN and EH 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 (T-0). Appropriate reference will be made in the installation AT plan referencing the IEMP 10-2 for emergency response procedures (T-0).

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, CBRN 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 IEMP 10-2, DCP, MCRP, AT, or IDP. Related contents of other plans should be referenced in the installation AT plan. These measures shall focus on mitigating vulnerabilities of personnel, families, facilities and materiel to terrorist use of CBRN 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, DoDI 6200.03, AFI 10-2603, AFI 10-2501; 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 CBRN and explosive 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 (T-0):

2.21.1.1. First Responders and Emergency Responders. Personnel responding to known or suspected CBRN and explosive 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 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. 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 Readiness and Emergency Management Flight, Public Health Emergency Officer, and Medical Readiness Office. These measures are implemented and synchronized with a corresponding FPCON measure for CBRN and explosive-specific threats **(T-0)**.

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 **(T-0)**.

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 **(T-0)**. 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 **(T-0)**.

2.21.5. Installation public health emergency response measures that are synchronized with FPCON levels shall be developed and implemented **(T-0)**.

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 (**T-0**). 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. Site-specific AT measures linked to an FPCON level and physical security actions shall be designated in accordance with DoDI 2000.16. When separated from the AT plan, specific AT measures linked to a FPCON and site-specific FPCON levels may be designated as FOR OFFICIAL USE ONLY IAW DoDM 5200.01, Volume 4, *DoD Information Security Program (T-0)*.

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, estimated completion date for full implementation, and installation OPR (**T-1**).

2.22.2.3.1. (**Added-AFMC**) Tenants on AFMC installations shall submit requests for FPCON waivers to the host installation and copy their owning MAJCOM.

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 (**T-0**). 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 (**T-0**). In addition to establishing procedures for raising FPCON levels, ensure procedures are developed for lowering FPCON levels (**T-2**). 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 31-117, *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.

2.22.2.5. (AFMC) All agencies assigned to an installation will develop site-specific FPCON measures for their unit. Ensure measures describe individual actions required for each facility to achieve each FPCON measure.

2.22.2.5.1. (Added-AFMC) Installation specific FPCON measures will be revised as necessary or within 60 days of any changes to DoD, GCC, AF, MAJCOM and/or local guidance changes.

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 (T-0). 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 installation AT plan shall be exercised annually and synchronized with other ID, EM, COOP and CARM program requirements (T-0). The installation shall coordinate with the Wing Inspection Team (WIT) to develop a comprehensive annual exercise program which provides for individual and collective AT proficiency training and realistic AT exercise scenarios (T-0). 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 (T-2). Site-specific FPCON measures from current FPCON through FPCON CHARLIE must also be exercised annually at all AF installations and separate facilities (T-0).

2.23.2.1. (Added-AFMC) AT exercises will have maximum participation by all base units, including tenants. The focus of the AT exercise is to detect deficiencies in executable plans and to identify corrective measures; consequently, simulations will be limited to the maximum extent possible. Simulations inhibit the accurate assessment of potential deficiencies an installation could only otherwise identify during implementation of that measure. Installations will incorporate local community EM/First Responders into installation exercises to test AFIMS integration with local application of NIMS as appropriate. Each AT exercise will be conducted and documented by the base WIT, providing a critique with findings, observations, and lessons learned.

2.23.3. AT exercise documentation shall be maintained for no less than two years by the WIT (T-0). Identified exercise findings will be presented to the ATWG and tracked/managed by the installation WIT until corrected or closed (T-2). 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> (T-0). AT training shall also be incorporated into pre-deployment training and exercises as required by the GCC (T-0). 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 follow table and rule guidelines located in the AF Records Disposition Schedule (RDS)

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).

2.24.1. (AFMC) Installation ATOs will identify how AT Level I-IV training is tracked and documented for their installation in the AT Plan.

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 (**T-0**). 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.

2.24.2.2. (AFMC) Installation reporting and corrective procedures for training deficiencies must be listed in the AT Plan. Method of training will be documented in and/or referred to in the AT Plan.

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.

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 (**T-0**).

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 a Level I - qualified instructor; completing the Force Protection computer-based training (CBT) course on the Advanced Distributed Learning System (ADLS); or by the Defense Technical Information Center (DTIC) at <https://atlevel1.dtic.mil/at> for individuals without access to NIPR, do not possess a CAC, or are not enrolled in DEERS. The ADLS—Force Protection CBT does not meet Department of State Chief of Mission (CoM) requirements for Level I - AT Awareness Training.

2.25.2.2.1. AF personnel assigned to a location where they will be under the responsibility of the Department of State 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 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 the Force Support Squadron 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 (**T-0**). The Force Support Squadron 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.

2.25.3. (**AFMC**) The method of training will be documented in and/or referred to in the AT Plan.

2.25.4. Level I - AT Awareness Training instructors must have completed an AF and/or Service-approved Level II - ATO Training course as outlined in Standard 26 (**T-0**). ATOs will maintain appointment letters of qualified instructors (**T-0**). As an interim solution, unit commanders in coordination with the ATO may certify and appoint qualified SMEs to conduct training if a certified instructor is not available. 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 AFSFC/SFOZ.

2.25.6. The AF's Level I - AT Awareness Training is built upon the minimum requirements 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. outlines the minimum required topics for AF Level I - AT Awareness Training (**T-0**).

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 Training and ATR Training.

2.26.1. Each AF installation and separate facility shall have a Level II-certified ATO appointed in writing (**T-0**). Level II – ATO training prepares and qualifies ATOs to perform their duties as AT program advisors and coordinators.

2.26.1. (**AFMC**) In coordination with Air Force Security Forces Center, AFMC ATPM may appoint a trainer to conduct AT Level II training IAW this AFI. Appointed instructors must meet the requirements of paragraph 2.26.2 of this AFI

2.26.1.1. Newly assigned ATOs shall complete training within 180 days of appointment (**T-2**). Deploying ATOs will complete training prior to deployment in accordance with line remarks. For both ATOs, Level II refresher training must be completed once every three years to maintain qualification (**T-0**). Refresher training may be accomplished by taking the Level II – ATO training refresher CBT available on ADLS or by attending a Military Department-approved Level II – ATO training course, either in residence or offered by an MTT.

2.26.2. Level II – ATO training course instructors should have at least two years of experience in the field of Antiterrorism and should 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, AF VAT, or Mission Assurance Assessment Teams to shadow those teams during an assessment. At a minimum, Level II – ATO training instructors will have completed the following qualification requirements and have task certifications documented in training records as appropriate (**T-2**):

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 and/or Service-approved Level II – ATO Training course.

2.26.2.3. CVAMP training.

2.26.3. Level II - ATO training must reflect current information on terrorism and AT program guidance. The Level II – ATO training course plan must also include measurable course objectives and evaluation methods to ensure student proficiency. The AF's Level II – ATO training is built upon and supplements the minimum requirements outlined in DoDI 2000.16, Standard 26, Table E3.T3. AT Level II – ATO training will be developed and reviewed annually by the MAJCOM sponsoring the course. Required course topics for AF Level II - ATO training are listed in Table 2.3. **(T-0)**. 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 compliance reviews during the first quarter of each calendar year.

2.26.4. ATRs should receive adequate training in order to carry out their assigned duties. ATR training should reflect current information on terrorism and AT program guidance. Training requirements may be developed by either the MAJCOM or the installation. Installation-developed ATR courses must be reviewed by the MAJCOM annually (T-2). Required minimum course topics for ATR training are listed in Table 2.4.

2.26.4.1. **(Added-AFMC)** As a minimum, Installation ATOs will ensure ATRs assigned to the installation receive initial training within 90 days of assignment via Defense Security Services (DSS) Antiterrorism Officer (ATO) Level II (www.cdse.edu/catalog/elearning/GS109.html) and locally developed training. At a minimum, local training will consist of items identified in Table 2.4. and, Random Antiterrorism Measures and processes for conducting them, creating unit site-specific FPCON Measures, exercise requirements, standoff procedures, and self-inspection program review checklist. ATOs and ATRs will maintain initial training documentation.

2.26.4.1.1. **(Added-AFMC)** Other recommended on-line courses are:

2.26.4.1.1.1. **(Added-AFMC)** National Terrorism Preparedness Institute Courses at <http://terrorism.spcollege.edu/Training/trainingOnline.aspx#Force>

2.26.4.1.1.2. **(Added-AFMC)** Defense Security Services Courses at www.cdse.edu/catalog/elearning/GS109.html

2.26.4.1.1.3. **(Added-AFMC)** Homeland Security Terrorism Prevention Courses at <https://www.preventivestrategies.net/>

Table 2.3. Level II – ATO 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

Table 2.4. ATR Training should 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 (**T-0**).

2.27.2. (**AFMC**) For situations where commanders or civilian equivalent, are not capable of receiving AT Level III training prior to assuming command, installation ATO must provide within 30-days of 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. (**AFMC**) The AFMC ATPM will accomplish this training during the AFMC Squadron Leaders Course (SLO). For commander/directors that did not attend the SLO, installation ATO will brief commanders/directors, to include tenant commander/directors utilizing the AT Level III slides on the AFMC AT EIM site. Installation ATO will provide a locally produced certificate to the commander/director. In addition, the Installation ATO will maintain a sign-in roster of all personnel trained IAW AFI 33-322, *Records Management Program*.

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 AFSFC/SFOZ 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 2.5. supplement Standard 27. A minimum of one hour is recommended to sufficiently address required topics.

Table 2.5. 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, other command and staff officers in 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 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 the GCC to orient all DoD personnel with AOR-specific information on AT protection (**T-0**). 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 (**T-0**).

2.29.2.1. (**Added-AFMC**) GCC information can be gathered on their respective NIPRNet/SIPRNet Websites. Family members can obtain country information at <https://www.fcg.pentagon.mil/>.

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 **(T-0)**. 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.

2.29.3.1. **(Added-AFMC)** Ensure that Air Force personnel travelling OCONUS receive CI and threat briefings. Only AFOSI provides CI briefings.

2.30. Standard 30: AT Resource Application.

2.30.1. Commanders shall assess risk against the standard and apply mitigation measures **(T-0)**. Where the resulting risk is still deemed too great, the countermeasure requirement shall be elevated using the PPB&E process **(T-0)**. Where applicable and in accordance with the MOU between the Department of State and the DoD, Overseas Security Support, coordination will be made through MAJCOMs or AF Components 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 **(T-0)**. 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 **(T-2)**.

2.30.5. Antiterrorism PEC 28047F is the primary funding source for manpower authorizations, AT equipment, procurement, and associated costs for the Air Force AT Program. AF/A4SX is the AF Program Element Monitor (PEM).

2.30.5.1. **(Added-AFMC)** AT funds (PEC 28047) will be dispersed for AT required training and to mitigate or correct vulnerabilities/concerns identified during VAs and/or those loaded in CVAMP.

2.30.5.2. **(Added-AFMC)** Work with CE programmers and/or SMEs to ensure that accurate cost are submitted. Ensure cost information is also submitted to installation via UFR supporting item entry. Ensure cost estimates for fixing CVAMP vulnerabilities/concern are located on the last line in the "discussion field." This will allow the data to be collected by AF/A4S for programming funds.

2.30.5.3. **(Added-AFMC)** CE programmers will provide cost data and/or estimates and ensure AT project(s) are entered into ACES. For projects to be considered for funding by AFMC, all requests must include the ACES project number, thus ensuring CE is aware of the project.

2.30.5.4. **(Added-AFMC)** AT projects will be incorporated into the installation's Integrated Priority List (IPL) for funding consideration. Wing leadership must emphasize appropriate prioritization for the program.

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. 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 **(T-0)**.

2.31.2. **(AFMC)** Installation ATOs will ensure the LMA/LVA team conducts the annual program review during the LMA/LVA. Ensure the final report addresses both the LMA/LVA and the PR.

2.31.3. Pre-deployment AT program reviews shall be conducted to ensure 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 **(T-0)**.

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 HHQ VAs, JSIVAs or Mission Assurance Assessments 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 headquarters' 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 **(T-0)**.

2.32. Standard 32: AT Program Review Teams.

2.32.1. AT program review assessment team guidelines shall be modeled upon DTRA's AT VA or Mission Assurance Assessment guidelines and include, at a minimum, compliance with the standards prescribed in this instruction, accepted TTPs, and AT best practices **(T-0)**.

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.).

TOD D. WOLTERS, Lt Gen, USAF
Deputy Chief of Staff, Operations

(AFMC)

DONALD E. KIRKLAND
Brigadier General, USAF
Director of Logistics, Civil Engineering and Force
Protection

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

- AF Doctrine Annex 3-10, *Force Protection*, 13 August 2014
- AF Doctrine Annex 4-0, *Combat Support*, 23 April 2013
- AFPD 10-2, *Readiness*, 6 November 2012
- AFPD 10-24, *Air Force Critical Infrastructure Program (CIP)*, 28 April 2006
- AFPD 10-25, *Air Force Emergency Management Program*, 28 April 2014
- AFPD 10-26, *Counter-Chemical, Biological, Radiological and Nuclear Operations*, 26 September 2007; Incorporating Change 1, 23 April 2013
- 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*, 7 July 2007; Incorporating Change 1, 29 October 2011
- AFPD 71-1, *Criminal Investigations and Counterintelligence*, 6 January 2010; Incorporating Change 2, 30 September 2011
- AFI 10-206, *Operational Reporting*, 11 June 2014
- AFI 10-208, *Continuity of Operations (COOP) Program*, 15 December 2011
- AFI 10-2501, *Air Force Emergency Management (EM) Program, Planning and Operations*, 24 January 2007; Incorporating Change 3, 29 April 2013; Corrective Actions Applied on 10 May 2013
- 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*, 23 April 2012
- AFI 14-119, *Intelligence Support to Force Protection (FP)*, 4 May 2012; Incorporating Change 1, 13 June 2014
- AFI 16-1402, *Insider Threat Program Management*, 5 August 2014
- AFI 23-302, *Vehicle Management*, 29 October 2007; Incorporating Change 2, 1 June 2009
- AFI 25-201, *Intra-Service, Intra-Agency, and Inter-Agency Support Agreement Procedures*, 18 October 2013
- AFI 31-101, *Integrated Defense*, 8 October 2009; Incorporating Change 27 March 2013
- AFI 31-117, *Arming and Use of Force by Air Force Personnel*, 29 June 2012
- AFI 31-113, *Installation Perimeter Access Control*, 26 January 2012
- AFI 38-101, *Air Force Organization*, 16 March 2011 (AFGM2.1, 15 Apr 2014)

AFI 38-201, *Management of Manpower Requirements and Authorizations*, 30 January 2014

AFI 65-601, Volume 1, *Budget Guidance and Procedures*, 16 August 2012

AFI 71-101, Volume 1, *Criminal Investigations*, 8 Apr 2011; Incorporating Change 1, 16 May 2013

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

AFI 71-101, Volume 4, *Counterintelligence*, 8 November 2011; Incorporating Change 1, 5 September 2012

AFI 90-201, *The Air Force Inspection System*, 2 August 2013; Incorporating Change 1, 10 March 2014

AFH 10-2401, *Vehicle Bomb Mitigation Guide*, 1 September 2006

AFMAN 10-246, *Food and Water Protection Program*, 27 May 2014

AFMAN 10-2503, *Operations in a Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive (CBRNE) Environment*, 6 July 2011; Incorporating Change 1, 31 May 2012

AFMAN 32-1084, *Facility Requirements*, 20 April 2012

AFMAN 33-363, *Management of Records*, 1 May 2008; Incorporating AFGM2014-01, 28 May 2014

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 5261.01G, *Combating Terrorism Readiness Initiatives Fund*, 2 December 2013

CJCSI 7401.01F, *Combatant Commander Initiative Fund (CCIF)*, 30 November 2012

CJCS Guide 5260, *A Self-Help Guide to Antiterrorism*, 10 June 2013

CJCS Pocket Card 5260, *Antiterrorism Individual Protective Measures*, July 2012

DoDD 3020.40, *DoD Policy and Responsibilities for Critical Infrastructure*, 14 January 2010; Incorporating Change 2, 21 September 2012

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

DoDD 6490.02E, *Comprehensive Health Surveillance*, 8 February 2012; Incorporating Change 1, 3 October 2013

DoDI 2000.16, *DoD Antiterrorism (AT) Standards*, 2 October 2006 Incorporating Change 2, 8 December 2006

DoDI 2000.12, *DoD Antiterrorism (AT) Program*, 1 March 2012; Incorporating Change 1, 9 September 2013

DoDI O-2000.22, *Designation and Physical Protection of DoD High-Risk Personnel*, 19 June 2014

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*, 17 November 2009; Incorporating Change 1, 15 October 2013

DoDI 6055.17, *DoD Installation Emergency Management (IEM) Program*, 13 January 2009; Incorporating Change 1, 19 November 2010

DoDI 6200.03, *Public Health Emergency Management Within the Department of Defense*, 5 March 2010; Incorporating Change 2, 2 October 2013

The DOD Antiterrorism Officer (ATO) Guide, November 2012

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

DoD 5200.08-R, *Physical Security Program*, 9 April 2007; Incorporating Change 1, 27 May 2009

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

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

JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010 (As amended through 15 August 2014)

UFC 4-010-01, *DoD Minimum Antiterrorism Standards for Buildings*, 9 February 2012; Incorporating Change 1, 1 October 2013

UFC 4-010-02, *DoD Minimum Antiterrorism Standoff Distances for Buildings*, 9 February 2012

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; Incorporating Change 1, January 2010

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

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

(Added-AFMC) USNORTHCOM Instruction 10-222, USNORTHCOM Force Protection (FP) Mission and Antiterrorism (AT) Program, 30 September 2014

(Added-AFMC) AFNORTH Instruction 10-222, Force Protection (FP Mission and Antiterrorism (AT Program for Air Forces Northern Area Of Responsibility, 8 January 2016

DoD Antiterrorism Vulnerability Assessment Benchmarks, 5 January 2011

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

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

Unified Command Plan, 17 December 2008

Prescribed Forms

None

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

AF Form 116, *Request For Deviation From Security Criteria*

(Added-AFMC) USNORTHCOM Instruction 10-222, *USNORTHCOM Force Protection (FP) Mission and Antiterrorism (AT) Program*, 30 September 2014

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

AFCEC—Air Force Civil Engineer Center

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

AF VAT—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
APHIS—Animal and Plant Health Inspection Service
BSAT—Biological Select Agents and Toxins
CARM—Critical Asset Risk Management
C-CBRN—Counter-Chemical, Biological, Radiological and Nuclear
C-NAF—Component-Numbered Air Force
CBRN—Chemical, Biological, Radiological, Nuclear
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
CONOPS—Concept of Operations
CONUS—Continental United States
CRP—Contingency Response Plan
CVAMP—Core Vulnerability Assessment Management Program
C-WMD—Countering Weapons of Mass Destruction
DBIDS—Defense Biometric Identification System
DBT—Design Basis Threat
DCIP—Defense Critical Infrastructure Program
DCP—Disease Containment Plan
DFARS—Defense Federal Acquisition Regulation Supplement
DFC—Defense Force Commander
DIA—Defense Intelligence Agency

DoD—Department of Defense
DoDD—Department of Defense Directive
DoDI—Department of Defense Instruction
DRU—Direct Reporting Unit
DTM—Directive Type Memorandum
DTRA—Defense Threat Reduction Agency
EDE—Explosive Detection Equipment
EH—Explosive Hazard
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
FPCON—Force Protection Condition
FPI—Force Protection Intelligence
FYDP—Future Years Defense Program
GCC—Geographic Combatant Commander
(Added-AFMC) GOCO—Government-Owned, Contractor-Operated
GSU—Geographically Separated Unit
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

IEMP—Installation Emergency Management Plan

IFC—Intelligence Fusion Cell

IPE—Individual Protective Equipment

JA—Judge Advocate

JP—Joint Publication

JSIVA—Joint Staff Integrated Vulnerability Assessment

LTA—Local Threat Assessment

MAA—Mutual Aid Agreement

MAJCOM—Major Command

MCRP—Medical Contingency Response Plan

MEF—Mission Essential Function

MEM—Medical Treatment Facility Emergency Manager

MILCON—Military Construction

MOA—Memorandum of Agreement

MOU—Memorandum of Understanding

MTT—Mobile Training Team

NAF—Numbered Air Force

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

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

PIR—Priority Intelligence Requirement

POM—Program Objective Memorandum
PPB&E—Planning, Programming, Budgeting and Execution
PPO—Protection Providing Organization
PPE—Personal Protective Equipment
PSVA—Personal Security Vulnerability Assessment
RAM—Random Antiterrorism Measure
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
SE/MA—Security Enterprise/Mission Assurance
SME—Subject Matter Expert
SOFA—Status of Forces Agreement
TACON—Tactical Control
TDY—Temporary Duty
TIC/TIM—Toxic Industrial Chemical/Toxic Industrial Material
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
USDA—United States Department of Agriculture
UTC—Unit Type Code
VA—Vulnerability Assessment
VAPO—Vulnerability Assessment Protection Option
VAT—Vulnerability Assessment Team
WIT—Wing Inspection Team
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/A4C.

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 CBRN.

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 CBRN 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 for domestic consequence management and the Department of State is the lead federal agency 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 lead federal agency.

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—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—US 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 US 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.

Explosive hazard—Any hazard containing an explosive component to include unexploded explosive ordnance (including land mines), booby traps (some booby traps are non-explosive), improvised explosive devices (which are an improvised type of booby trap), captured enemy ammunition, and bulk explosives. (JP 1-02 and JP 3-15)

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 CBRN 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).

Force Protection Condition (FPCON)—A DoD-approved system standardizing the Department's identification, recommended preventive actions and responses to terrorist threats against US 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—An overall assessment by a higher headquarters of how an organization is managing its AT program, including management and compliance efforts by subordinate organizations.

Insider Threat—The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities (AFI 16-1402).

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 US 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 protective service detail 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.

(Added-AFMC) Semi-annual—Occurs every half year (6-months). However, due to unforeseen circumstances this may be adjusted to a month prior to, or a month after the 6-month mark.

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 Department of State 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 US 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 (ATR)—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 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 locally-developed measures address 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. (AFMC)AF/AFMC “added” measures will not: Be “implied” when an AFNORTH FPCON baseline change is done. All AFNORTH/AFMC FPCON changes will state specific AF/AFMC “added” measures, if deemed necessary. However, if a HHQ FPCON measure has an associate AF/AFMC “modified” measure; it will be implemented; even if not specifically stated in the AFNORTH/AFMC FP Directive.

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) apprised 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 linked to an FPCON level and physical security actions shall be designated in accordance with DoDI 2000.16. When separated from the AT plan, specific AT measures linked to a FPCON and site-specific FPCON levels may be designated as FOR OFFICIAL USE ONLY, IAW DoDM 5200.01, Volume 4.

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

A2.1.7. The CBRN-related FPCON measures contained in this publication are not all inclusive. Additional CBRN FPCON measures are in the AF Civil Engineer Center (AFCEC) IEMP 10-2 tool at https://cs3.eis.af.mil/sites/OO-EN-CE-A6/21340/OO-EN-CE-52/iemp_10-2/SitePages/Home.aspx 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 CBRN FPCON measures applicable to their location.

A2.1.8. **(Added-AFMC)** TWGs at all levels will be formed to determine if higher measures are required for their specific AORs. Notify AFMC Command Center and AFMC ATPM of findings and recommendations.

A2.1.9. **(Added-AFMC)** Immediately upon notification of a decrease in FPCON, form TWGs at all levels to determine flexibility of decreasing the FPCON within your AOR. Prior to decreasing HHQ directed FPCONs locally, ensure you have obtained HQ AFMC/TWG recommendations, as the HQ AFMC/CC may not decrease FPCONs. Notify AFMC ATPM of findings and recommendations.

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 checks 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.

A2.2.2.1. (AFMC) Measure NORMAL 2.1 (Modified): Commercial delivery and/or contract vehicles will be searched for explosives and/or contraband IAW AFMAN 31-113. Commercial delivery and contract vehicles are defined as a 15-passenger van or have an enclosed box behind the cab of the vehicle, which cannot be viewed by the Entry Controller.

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.

A2.2.5. (AFMC) Measure NORMAL 5 (Modified): Conduct a minimum of 3 RAMs per day IAW Standard 14 of this AFI.

A2.2.6. Measure NORMAL 6 (AF Added): Conduct 100% —hands onl 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.

A2.3.2.1. (AFMC) Measure ALPHA 2.1 (Modified): Post signs at all points that lead from off-installation/separate facility onto the installation/separate facility.

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, IEMP 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 CBRN 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.

A2.4.1.1. (AFMC) Measure BRAVO 1.1 (Modified): Post signs at all points that lead from off-installation/separate facility onto the installation/separate facility.

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.

A2.4.1.2. (AFMC) Measure BRAVO 1.2 (Modified): Conduct a minimum of 4 RAMs per day IAW Standard 14 of this AFI.

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

A2.4.1.4. Measure BRAVO 1.4 (AF Added): Verify the interoperability of CBRN response procedures with local community resources, to include activities outlined in the IEMP 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 CBRN 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).

A2.4.7.1. (AFMC) Measure BRAVO 7.1 (Modified): Conduct 100% identification checks on all vehicle occupants 18 years old and older.

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.

A2.4.19. (AFMC) Measure BRAVO 19 (Modified): Close all non-essential flightline access control points. Post flightline Entry Control Points (ECP) with either SF augmentees and/or owner/user personnel; owner/user personnel are more familiar with authorized personnel in the area. Consider selective arming of personnel based on threat and operating environment.

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 CBRN 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.

A2.5.1.1. (AFMC) Measure CHARLIE 1.1 (Modified): All personnel entering the installation must be properly proofed, vetted and provided an authorized entry credential.

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 CBRN threat exists, ensure the Disaster Response Force and, if permissible, local authorities are briefed on the threat.

A2.5.1.2. (AFMC) Measure CHARLIE 1.2 (Modified): Post signs at all points that lead from off-installation/separate facility onto the installation/separate facility.

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.

A2.5.1.3.1. (Added-AFMC) Measure CHARLIE 1.3 (Modified): Conduct a minimum of 5 RAMs per day IAW Standard 14 of this AFI.

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.

A2.5.4.3. (Added-AFMC) Measure CHARLIE 4.3 (Added): As threat dictates, post installation ECP overwatch positions. The overwatch position will employ suitable devices that have the capability to impede or defeat the threat.

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 CBRN 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 CBRN threat exists, ensure all shortages of C-CBRN 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 CBRN 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-US 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.

A2.5.17. (Added-AFMC) Measure CHARLIE 17 (Added): Implement procedures for limiting installation access (curtailment plan) to mission essential personnel only.

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.

A2.6.1. (AFMC) Measure DELTA 1 (Modified): Post signs at all points that lead from off-installation/separate facility onto the installation/separate facility.

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.

A2.6.7.1. (**Added-AFMC**) Measure DELTA 7 (Added): Close non-essential operations and services such as Commissary, AAFES, Food Court, etc.

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

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 US targeting to include the movement of key operatives, final intelligence collection and movement of weapons to the target vicinity. Less threatening actions are contingency planning, training and logistical support. Activities that would make the group less likely to attack, such as robust fund raising or effective safe haven are considered. Whether the group has recently been disrupted by arrests or strikes on training camps will reduce the threat, at least in the short term.

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 US and the quality of the reporting on terrorist groups in the country. A key element is whether there is a DoD presence and if so the type, size, location, political sensitivity and if temporary, its duration. It is also important to consider if the group is focused on DoD as its primary target for anti-US attacks. Another part of this factor is the overall political, economic and military stability of the country and its effect on the ability of a group to attack.

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 AFD 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 28047F 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.

A4.4.3. (AFMC) CCIF requests are not submitted through CVAMP; however, the emergent requirement must be in CVAMP. Installations submit request via package through the Center to AFMC ATPM. Package will be forwarded to AFNORTH and USNORTHCOM by the MAJCOM.

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. 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 Enterprise and Analysis 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. 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. Additionally, they can provide field assessments to assist in identifying the optimal solutions to meet 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 650 7013.

ANG, NGB/A7S, Andrews AFB, MD. Phone: 240-612-9592, DSN, 612-9592, sfs.ato@ang.af.mil

PACAF Regional Training Center, 736th Security Forces Squadron, Andersen AB, Guam. 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, Germany. 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 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 the deviation is being made specifically states it is not necessary.

A6.5. (AFMC)Deficiencies which cannot be explained in a word picture will: Be accompanied by photographs, maps, diagrams or other pictorial aids. All deviations must include an estimated get-well/completion date (if known).

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.

A6.5.1.1.1. **(Added-AFMC)** All deviation requests will be routed through the appropriate Center CC for coordination prior to submission to AFMC.

A6.5.1.1.2. **(Added-AFMC)** Deviations related to physical security requirements will be maintained by the installation SF unit.

A6.5.1.1.3. **(Added-AFMC)** Deviations related to minimum UFC AT Standards for Buildings will be submitted and managed by the BCE or CES designated representative. The requestor of the deviation may be someone other than BCE, but the submission and management must be BCE. The installation staffing package will include the installation ATO as a coordinating official prior to submission to Installation Commander for signature. Under mitigation section, total projected costs to alleviate the deviation will be included. A copy of the deviation request shall be provided to the installation ATO.

A6.5.1.1.4. **(Added-AFMC)** NCI 10-222 requires no deviation request for standoff requirements

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 Civil Engineering and/or A7P and MAJCOM ATPM will coordinate (at minimum).

A6.5.3. (AFMC) The deviation request for minimum UFC AT Standards for Buildings will be submitted to AFIMSC Det 6, as the subject matter expert for UFC issues. AFIMSC Det 6 will staff recommendation to AFMC/CV for approval/disapproval.

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.

A6.6.1.3. (AFMC) AFMC Security Forces will provide copies of approved UFC deviations to AFIMSC, AF/A4S and AFNORTH.

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. (AFMC)Compensatory measures shall : Be instituted for each deviation and must be implemented immediately upon detection. If appropriate, one compensatory measure may suffice for more than one deviation.

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-AFMC)
UNIT PROGRAM REVIEW (UPR)

A8.1. (AFMC) In accordance with AFI 10-245, AFMCSUP, Antiterrorism, para 2 9.3.15: Installation/wing ATOs will use the following checklist when conducting an UPR. Installation and wing ATOs may augment this checklist with additional criteria.

A8.1.1. (AFMC) Does unit have a primary & alternate wing/unit ATO/ATR appointed in writing? (paras 2.9.1 and 2.9.1.3.)

A8.1.2. (AFMC) Has wing/unit ATO/ATR scheduled initial training with the installation ATO within 90 days of appointment? (para 2.26.4.1.)

A8.1.3. (AFMC) Has commander or civilian equivalent appointed, in writing, a primary and alternate wing/unit ATO/ATR in the grade of E-5 or above to include civilian equivalent (GS-5)? If not, has the commander or civilian equivalent identified why they were unable to meet the minimum requirements in the appointment letter? (paras 2.9.1. and 2.9.1.3.)

A8.1.4. (AFMC) If required, did unit SMEs participate in the annual AT assessment and risk management process? (paras 2.9.3.10. and 2.9.4.12.)

A8.1.5. (AFMC) Does unit ensure Military Service family members (14 years of age or older) traveling beyond CONUS on official business receive AT Level I training/refresher (e.g., PCS move)? (para 2.25.3.)

A8.1.6. (AFMC) Does unit have provisions to ensure members traveling OCONUS receive appropriate training? (paras 1.3.1. and 1.3.3.)

A8.1.7. (AFMC) Have all unit personnel been provided information pertaining to the Eagle Eyes program to include incidents, what to report and reporting procedures? (para 1.2.5.1.)

A8.1.8. (AFMC) If required, has your Wing or Group Commander (O-6s) or civilian equivalent attended the Level IV training course? (para 2.28.2.)

A8.1.9. (AFMC) Has your Unit Commander or civilian equivalent received Level III training? (para 2.27.2.)

A8.1.10. (AFMC) Does unit have a system to track and document AT levels I through IV training? (para 2.24.2.)

A8.1.11. (AFMC) Has unit developed site-specific FPCONs? (para 2.22.2.5.)

A8.1.12. (AFMC) Do these measures describe in detail individual actions required for each unit facility to achieve each FPCON measure? (2.22.2.5.)

A8.1.13. (AFMC) Have instructions on door-guard responsibilities been written and trained to personnel responsible for holding these duties during RAMs and higher FPCONS? (para 2.9.4.11.)

A8.1.14. (AFMC) Does unit participate in the installation RAM program as required? (paras 2.9.3.12. and 2.9.4.4.)

A8.1.15. (AFMC) Has Unit Commander or civilian equivalent published a unit antiterrorism instruction for personnel and areas under their control? At a minimum, the

instruction will include wing/unit ATO/ATR duties and responsibilities and procedures for bomb threats, active shooters, suspicious mail, suspicious packages, mail handling procedures and building and fire evacuations? (para 2.9.4.10.)

A8.1.16. (AFMC) Is Unit Antiterrorism Instruction reviewed annually or when changes occur? (para 2.9.4.10.)

A8.1.17. (AFMC) Does wing/unit ATO/ATR have a parking plan to move containers and vehicles away from the facility IAW UFC 4-010-01? (para 2.9.4.10.)

A8.1.18. (AFMC) Does wing/unit ATO/ATR attend specified work group meetings as published in this guide? (para 2.9.3.15. and 2.9.4.13.)

A8.1.19. (AFMC) Has wing ATO attended a formal AF approved AT Level II course within 180 days of appointment, if applicable? Or has the wing ATO been scheduled to attend? (para 2.26.1.1.)

Attachment 9 (Added-AFMC)**ANTITERRORISM APPOINTMENT LETTER TEMPLATE (INSTALLATION ATO)**

A9.1. (AFMC) Shall be on installation letterhead.

A9.2. (AFMC) Appointment letter shall identify the following:

A9.2.1. (AFMC) Paragraph 1 will include the following statement, "In accordance with AFI 10-245, *Antiterrorism*, para 2.9.1., I appoint the following personnel as primary and alternate installation Antiterrorism Officers (ATO) for XXXX Center/AFB/Plant/Lab/Site. The alternate ATO will perform the primary duties and responsibilities for the primary ATO. As the installation ATOs, they are authorized to update and perform roles as the ATO, Resource Manager, Assessor, and Commander (identify some, none, or all permissions) in the Core Vulnerabilities Assessment Management Program (CVAMP)." NOTE: The DFC will be listed as the installation ATO and the person fulfilling their duties and responsibilities will be listed as the alternate ATO.

A9.2.2. (AFMC) Paragraph 2 will identify the Name, Grade and Security Clearance level of the primary and alternate ATOs.

A9.2.3. (AFMC) Paragraph 2a will identify the reason for appointing a contractor as the installation's ATO instead of a military or government employee.

A9.2.4. (AFMC) Paragraph 3 will list contact information for the primary and alternate ATOs (e.g., NIPR/SIPRNET e-mail addresses, duty phone number, and off-duty).

A9.2.5. (AFMC) Paragraph 4 will list the latest graduation date from AT Level II, ADLS AT Level II refresher training, if applicable and Security Engineering Design courses, if attended.

A9.2.6. (AFMC) Paragraph 5 will state "This letter supersedes all previous letters same subject."

A9.2.7. (AFMC) Letter must be signed by Installation Commander. NOTE: Upon receipt of the ATO appointment letter, ATPM, as administrator for CVAMP, will update authorized permissions.

Attachment 10 (Added-AFMC)**ANTITERRORISM APPOINTMENT LETTER TEMPLATE (WING ATO/UNIT ATR)**

A10.1. (AFMC) Shall be on letterhead.

A10.2. (AFMC) Appointment letter shall identify the following:

A10.2.1. (AFMC) Paragraph 1 will include the following statement, "In accordance with AFI 10-245, *Antiterrorism*, para 2.9.1.1 and AFI 10-245_AFMC SUP, para 2.9.1., I appoint the following personnel as primary and alternate Antiterrorism Officers (ATO)/Antiterrorism Representative (ATR) for XXXX (wing/unit).

A10.2.2. (AFMC) Paragraph 2 will identify the Name, Grade and Security Clearance level of the primary and alternate ATO/ATRs.

A10.2.3. (AFMC) Paragraph 2a will identify the reason for appointing a contractor or a military/civilian (not meeting the rank requirement by the AFI) as the wing/unit ATO/ATR.

A10.2.4. (AFMC) Paragraph 3 will list contact information for the primary and alternate ATOs (e.g., NIPR/SIPRNET e-mail addresses, duty phone number, and off-duty).

A10.2.5. (AFMC) Paragraph 4 will list the latest graduation date from AT Level II, ADLS AT Level II refresher training, if applicable and Security Engineering Design courses, if attended.

A10.2.6. (AFMC) Paragraph 5 will state "This letter supersedes all previous letters same subject."

A10.2.7. (AFMC) Letter must be signed by Commander or equivalent for that agency.