



COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

OPR: HQ AMC/SFOF (MSgt Joseph M. Bovair)

Certified by: HQ AMC/SF
(Col James R. Hutchison)

Supersedes AFI 31-210, AMCS1, 1 June 2000

Pages: 44

Distribution: F

AFI 10-245, 21 June 2002, is supplemented as follows. This publication consolidates the procedures and criteria that support AMC's AT Program. It applies to all AMC installations and those AMC units tenant on other command or service installations. It does not apply to AMC-gained Air Force Reserve Command (AFRC) or Air National Guard (ANG) units; operational control of the AFRC and ANG gained units' AT program remains with the AFRC and/or ANG. All AFRC and ANG units required to report AT program status/measures will continue to process their information through their headquarters. Gained AFRC and ANG units may utilize this supplement to assist their AT program management. Send recommended changes to this publication via **AF Form 847, Recommendation for Change of Publication**, to HQ AMC/SFOF, 102 East Martin Street, Room 230N, Scott AFB, IL 62225-5318.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed.

Adopts the term AT Advisor in lieu of AT Officer and/or AT NCO, as the primary individual(s) for Anti-terrorism (AT) related issues. Places the Wing AT Advisor position at the Wing Plans Office (XP). Additionally, replaces the acronym CINC with "geographic commander (CDR)".

1.1. **AMC AT Program.** The AMC AT program enhances the Department of Defense and Air Force programs of deterrence designed to blunt terrorist acts against personnel and resources by providing timely guidance on collecting and disseminating threat information. This will be accomplished by providing training to all command members, developing comprehensive plans, allocating funds, and implementing defensive measures. AMC/CC established a 3-tier AT/FP Corporate Structure, consisting of a Force Protection Working Group (FPWG), Force Protection Board (FPB) and Force Protection Council (FPC) that addresses all AMC Force Protection (FP) matters and policy. See paragraph **2.1.1.14** for additional guidance on the AT/FP Corporate Structure.

1.1.2. AT Responsibility. AT is an installation commander responsibility and must be thoroughly integrated into every unit attached to the installation, to include tenants, Sister Services, and attached agencies (i.e., AAFES, DECA, TRICARE, etc).

1.1.2.1. (Added) The program is an integrated effort where all units and installation commanders must have the mindset combating terrorism is not solely the responsibility of the Security Forces (SF). Security Forces are merely one component of a comprehensive, successful team effort.

1.1.3. Countering the Threat. Each AMC installation will establish an AT/FP decision-making body to fully integrate and coordinate AT/FP actions. Key functional membership for this decision-making body, at a minimum, will include: Air Force Office of Special Investigations (OSI), Communications (SC), Civil Engineering (CE), Intelligence (IN), Judge Advocate (JA), Operations, Security Forces (SF), Financial Management (FM), and Surgeon General (SG). This may be accomplished by enhancing the Installation Security Council (ISC) or by establishing a separate Force Protection Working Group (FPWG). The installation threat-working group (TWG) should maintain its unique functions. See also paragraph 2.1.1.14 in the AFI.

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

2.1.1.3.3. AMC/SF monitors Responsibility Center/Cost Center (RCCC) 1001B4 (Force Protection Board Fund), and coordinates funding submissions for AT/FP initiatives with AMC functional experts for FPWG/FPB approval.

2.1.1.3.3.1. (Added) The Force Protection Board (FPB) Fund is primarily used to operate the command's AT/FP Program. It funds (but is not limited to) AMC Vulnerability Assessments (VAs), AMC FP Staff Assistance Visits, oversight for Joint Staff Integrated Vulnerability Assessment (JSIVA), Air Force VAs, FP audits by GAO, AF Audit Agency, US Transportation Command (USTRANSCOM) or other agency, and AT/FP related training/schools. Requests for utilization of funds are approved by the FPWG and/or FPB. See paragraph **2.2.1.4.3. (Added)** for additional guidance on the FPB Fund.

2.1.1.3.3.1.1. (Added) The FPWG approves all requests for funding under \$10K. Submissions can be forwarded for review via email, SSS or during a FPWG meeting. Requests not receiving unanimous approval are forwarded to the FPB chairman for resolution.

2.1.1.3.3.1.2. (Added) The FPB approves all requests for funding over \$10K. Submissions can be forwarded for review via email, SSS or during a FPB meeting. The FPB chairman should resolve conflicts in coordination; however, he/she has final approval authority. Any member of the FPB may raise the conflict to the FPC chairman via an officially staffed SSS.

2.1.1.3.5. Conducts AMC Vulnerability Assessments as outlined in paragraph 2.26. AMC SFOF is the primary POC for scheduling/coordinating JSIVA and AF VAs with the installation AT Advisor and coordinates all AT/FP visits with the AMC IG gatekeeper as far in advance of the visit as possible.

2.1.1.4. AMC/SG provides core members to the AMC FPC, FPB, and FPWG, as required. AMC/SG provides a Health Service Support representative (Bioenvironmental Engineer or Public Health) as a core member of the AMC Vulnerability Assessment Team (VAT). Additionally, AMC/SGP is a primary member of the AMC Threat Working Group (TWG).

2.1.1.9. AMC/CE provides core members (Engineering and Readiness) to the AMC FPC, FPB, and FPWG, as required. AMC/CE provides readiness and infrastructure engineers to support the AMC VA team.

2.1.1.13. AFOSI Region 3 provides core members to the AMC FPC, FPB, and FPWG, as required. AFOSI Region 3 provides a fully qualified terrorist options specialist to support the AMC VAT. Additionally, AFOSI Region 3 is a primary member of the AMC TWG.

2.1.1.13.8. (Added) AFOSI Region 3 chairs the CONUS Threat Working Group (CTWG) weekly or as determined by the membership. Members include, but are not limited to: OSI, SF, SG, and IN. The CTWG evaluates CONUS threat information and recommends changes in FPCONs to AMC/CC.

2.1.1.14. AMC/CC established the 3-tiered AT/FP corporate structure. AMC/SF is the OPR and the executive agent for AMC AT/FP matters and policy. AMC/SFOF coordinates all functions of the corporate structure. AMC/CV is the chair for the Force Protection Council (FPC). AMC/SF is the OPR and chair for the Force Protection Board (FPB), and AMC/SFO is the OPR and chair for the Force Protection Working Group (FPWG). Minutes will be forwarded to working group members who will forward them to their respective 2-digit board member.

2.1.1.14.1. (Added) Every AMC directorate and the TACC provides membership to the AMC FPC, FPB, FPWG, as required. Exceptions are AMC/HC, AMC/HO, and AMC/TE. AMC/RE attends as required by the agenda item(s).

2.1.1.14.2. (Added) The FPC meets annually or as directed by AMC/CV. FPC business can be accomplished via SSS when schedule conflicts preclude holding an FPC meeting.

2.1.1.14.3. (Added) The FPB meets bi-annually or as determined by the FPC and/or FPWG. Issues forwarded from the FPWG may require an out-of-cycle meeting. If possible, business/issues should be conducted via SSS to accommodate conflicts in schedules and expedite coordination.

2.1.1.14.4. (Added) Installation commanders will establish a FPWG to include functional representatives listed in paragraph 2.1.1.14 of the AFI. Membership and specific functions will be added to the installation AT Plan and a supplement to this publication.

2.1.1.14.5. (Added) AMC/DS will provide membership to the 375 AW Force Protection Working Group and Installation Security Council (ISC). AMC/DS is the POC for all AMC headquarters AT/FP matters as a tenant organization of Scott AFB. AMC/SF retains all higher headquarters AT/FP responsibilities as the MAJCOM POC.

2.2. AMC/SF is the OPR for this supplement, which implements the Air Force AT program within AMC.

2.2.1. Installation/Site Commanders will provide HQ AMC/SF a copy of their supplement within 120 days from the date of this supplement, and as changes occur thereafter.

2.2.1.4. The ISC and/or Force Protection decision-making body should consider identified vulnerabilities in Vulnerability Assessment Management Program (VAMP), when the installation commander's priority requirements list is developed for AT/FP funding submissions.

2.2.1.4.1. AT Funding. Installation commanders should address vulnerabilities identified in local or Higher Headquarters Vulnerability Assessments. Installation AT Advisors collect and prioritize vulnerabilities that require funding. The Vulnerability Assessment Management Program (VAMP) provides a tool for tracking, reporting, and prioritizing vulnerabilities. Through coordination with the Installation FPWG, AT Advisors and installation commanders should prioritize these vulnerabilities and submit

unfunded requests through their local FMB to HQ AMC/FMB utilizing Responsibility Center/Cost Center (RCCC) 104380 (Antiterrorism). A copy of unfunded requirements should also be forwarded to AMC/SFXP and AMC/SFOF.

2.2.1.4.2. CbTRIF Funding. Submit emergent CbTRIF submissions to HQ AMC/SFX twice a year (1 Sep and 1 Jan) IAW CJCS 5261-01B, Enclosure B. All emergent requirements must have an approved, executable, and exercised AT Plan prior to submitting a CbTRIF request. The installation FP decision-making body, e.g., ISC, should review all CbTRIF submissions and approve before submission to HQ AMC/SFX. Action officers preparing the CbTRIF submissions must research funding amounts, and ensure the requested amounts are firm and can be obligated within 90 days upon receipt of funding. Ensure budget requests have a direct AT/FP application with wide-ranging impact. Emergency requirements can be submitted anytime during the fiscal year using Enclosure B of CJCS 5261-01B. Emergency requirements are unanticipated requirements created by a combination of circumstances or the resulting state that requires immediate action to prevent, deter, or respond to a terrorist act.

2.2.1.4.3. (Added) Force Protection Board (FPB) Funding. The FPB receives funds from AMC/CC to operate the command's AT/FP Program. The fund is BA02 (O&M) dollars. On occasion, AMC/SF (through the FPWG and FPB) may request installation AT Advisors and/or AMC directorates, submit proposals to obligate portions of this fund, throughout the calendar year.

2.2.1.4.3.1. (Added) At no time, should an installation commander or AT Advisor consider this fund for their AT/FP projects, future funding, or supplemental funding sources, nor should it be utilized to replace un-funded requirements. Funds requests should only be submitted if the FPWG/FPB initially asked for submissions. At no time, should a unit submit proposals without a prior request by the AMC FPWG/FPB.

2.2.1.4.3.2. (Added) If such a request is made, installation submissions should be coordinated by the FPWG, however all submissions must be approved by the Installation Commander, as a minimum. Submissions must be within the allocated dollar amount, otherwise, it will not receive consideration by the FPWG or FPB.

2.2.1.4.3.3. (Added) Format to submit end of year proposals for FPB Funds should be IAW **Attachment 9 (Added)**, of this supplement.

2.2.1.4.4. (Added) Baseline Equipment Data Assessment List (BEDAL) Funds. Non-Medical BEDAL funding is administered through HQ USAF/ILEX centrally managed PE 27574. HQ AMC/CEXR provides program element oversight, consolidates all Non Medical BEDAL requirements, and advocates for BEDAL funding for the command. Installations will use their Readiness Working Group to determine priority requirements for EOD, Fire, HAZMAT, Readiness, and Security Forces BEDAL equipment. Installation CE Readiness flights will consolidate requirements and submit them to HQ AMC/CEXR for funding.

2.2.1.5. Plan for physical security of new facilities through the Base Civil Engineer (BCE) office and the ISC.

2.3.1. Installation/site commanders have operational responsibility for AT/FP for all units and individuals whether permanently or temporarily assigned. In accordance with Joint Pub 3-10, *Doctrine for Joint Rear Area Operations*, Chapter II, paragraph 3b, tenant AMC units of another MAJCOM or service installations will comply with the requirements of the host AT/FP program. Tenant commanders maintain overall responsibility for their command's physical security and AT/FP planning not provided by the host installation.

2.3.1.1. (Added) Air Mobility Warfare Center (AMWC). The AMWC, an AMC DRU, is located at Ft Dix, an active Army installation. Therefore, as a tenant of Ft Dix, the center assumes the Provost Marshall and/or Commander, Ft Dix's FP measures and posture. The AMWC receives vulnerability assessments as a tenant of Ft Dix. The AMWC provides AT/FP Level II training by formal school and/or mobile training team (MTT) visits to AMC installations.

2.3.1.2. (Added) Defense Courier Stations (DCS). Defense Courier Stations are AMC DRUs, located on US military installations worldwide. DCS assumes the FP measures and posture of the parent (host) organization. In the absence of a host organization, DCS assumes the FP posture of the geographic CDR. DCS is afforded AT/FP Level II training from AMWC through formal MOA between AMC/SF and DCS/JS (Directorate of Plans and Operations).

2.3.4.1. Installation-wide antiterrorism exercises (both operational and command post) will be conducted at the installation commander's discretion, but no less than annually. The exercises will be used to test and evaluate the installation's ability to respond to the local terrorist threat. Exercises will test a broad range of required FPCON actions specified within the installation's local plans and may be combined with other base exercises such as a MARE, BROKEN ARROW, etc. Installation commanders will document a review of their Installation AT Plan on an annual basis or within 60 days of assuming command. Installation AT Advisors must maintain the commander's review with the AT Plan. A copy of the commander's review must be forwarded to AMC/SFO within 15 days of completion. See also, AMC Sup 1, AFI 31-101, paragraph 4.10.

2.3.4.2. Installations are tasked through the public affairs program, with providing periodic AT/FP awareness information on terrorist threats and personnel protection principles and techniques to the base populace. This may be satisfied using cable access station, base newspaper articles or flyers distributed at accessible points throughout the installation. Incidents of terrorism and crime will generate external media interest. In response to queries concerning a possible or real terrorist threat at a particular activity, installation, or community, the commander may acknowledge that increased security measures have been or will be taken without going into specific details regarding the measures being taken. In other words, it may be appropriate and operationally sound to acknowledge the obvious. For example, increased security measures such as additional guards at the gate and/or more stringent identification checks are usually obvious to the public, and acknowledgement may serve to send a positive message of increased readiness. Commanders must exercise care and prudent judgment in any discussion of these or other security measures to preclude revealing tactics and techniques that an adversary could exploit. Discussion of site-specific FPCON measures IAW the Installation AT Plan are classified confidential IAW paragraph 2.13 of the parent AFI.

2.3.4.5. (Added) . AMC/LGTB provides the AMC Corporate Structure specific guidance for passenger/cargo force protection related policy as it relates to TSA regulations and policy. All TSA related incidents and policy will be coordinated with AMC/LGTB.

2.4. The AMC Threat Working Group (TWG) is the command focal point for coordinated threat analysis and FP recommendations for AMC operations in high-risk locations. The TWG meets daily to assess potential threats affecting AMC operations using a six-step Operational Risk Management (ORM) process to review hundreds of weekly missions transiting secure launch, monitor, and RAVEN required locations around the world. The AMC Virtual Risk Assessment Database (VRAD) is the TWGs most widely used product and is available via AMC Intelligence's classified website

<http://www.amcin.scott.af.smil.mil>. The VRAD contains published analysis detailing threats and FP recommendations for locations where AMC operates. Included in each airfield risk assessment is

approved AMC DO policy used for planning and executing missions. Requests to deviate from established policy are reviewed by the TWG, on a case-by-case basis. The final approval authority is either the AMC Director of Operations (DO) or the AMC Tanker/Airlift Control Center (TACC) Commander, based upon when the mission enters into execution. Waiver requests should be submitted electronically via AMC Intelligence's classified website listed above.

2.4.1. Ensure local and host nation support planning efforts consider Threat Levels 1 and 2 (AFI 31-301, *Air Base Defense*), as well as the known criminal threat in the immediate area of the installation. Installation/Site Commanders will ensure all agreements for local emergency support; e.g., fire, police, health service support, etc., are formally coordinated for their installations/sites. Review of agreements is a part of the AT/FP vulnerability assessment process.

2.5.1. Installation commanders will designate, in writing, a full-time staff officer to supervise, inspect, exercise, review, assess and report on the AT program at the installation. Installation commanders will appoint and maintain a full-time Antiterrorism Advisor and consider a full-time staff.

2.5.1.1. AT Advisors must be trained in AT procedures as described in DoDI 2000.16 and DOD O-2000.12-H. Training will include attendance at a parent AT Level II MAJCOM approved course. Courses that specialize in Air Force installation vulnerability assessments are encouraged. This training is required within 120 days of appointment to the position. When possible, the person(s) appointed should remain in the position for at least 18 months.

2.5.1.2. (Added) Every effort should be made to ensure the AT Advisor is not TDY within 120 days of a higher headquarters vulnerability assessment.

2.5.2. The AMC FPWG points of contact (POCs) will coordinate (as determined by the Contract Owner) on all contracts and/or Statements of Work (SOW). The process is as follows:

2.5.2.1. (Added) All FPWG members email addresses are maintained by AMC/SFOF, in a database updated as significant changes occur. Each FPWG member will maintain this address group and forward contracts/SOWs that originate in their area of expertise.

2.5.2.2. (Added) The contract owner and/or FPWG member will determine, based on the nature of the contract, who should provide coordination on the electronic SSS. The contract owner or FPWG member then forwards the SSS to all FPWG members in the address group, regardless of required coordination. FPWG members identified as requiring coordination must provide their 3 or 4 digit coordination directly to the contract owner (POC identified on the SSS).

2.5.2.3. (Added) The contract owner will resolve issues with directorates who non-concur or do not provide coordination. All efforts to resolve conflict from the coordination process should be handled by the contract owner.

2.5.2.4. (Added) Upon completion of all coordination action, the contract owner will then provide a completed SSS to AMC/SFOF via email. AMC/SFOF will establish a cover letter for the FPWG chairman (AMC/SFO) to sign, indicating a FPWG review has taken place on the specific contract. Upon signature, a copy will be provided to the contract owner.

2.5.2.5. (Added) AMC/SFOF will maintain copies of all cover letters signed by the FPWG chairman. The specific contract owner will maintain copies of all coordination actions, along with the signed letter from the FPWG chairman.

2.5.2.6. (Added) AMC/JA review IAW the above process will occur prior to contract award and not during FPWG review, to alleviate redundant review requirements.

2.5.3. AT Plans will be assessed during higher headquarters program reviews as identified in Standard 26 to DoDI 2000.16 and paragraph 2.26 to AFI 10-245. Plans shall address areas outlined in paragraph 2.2.1. Commanders are encouraged to use the DD ATFP (previously J-34) AT/FP Installation Planning Template CDROM in developing/revising their installation plans.

2.5.4. Installation commanders will report Air Force Strategic Plan, Vol. 2, Performance Plan FP Performance Measures 2.A.12, Antiterrorism/Force Protection Program, semi-annually, no later than 1 Apr and 1 Oct of each year to AMC/SFOF. Installation commanders must coordinate on the report prior to release to AMC/SFOF. Installation AT Advisors should be afforded minimal levels of staffing in order for the Installation commander to provide coordination within the suspense dates above. Continue reporting during emergency conditions.

2.5.4.1. Reporting periods for both FP Performance Measures are 1 Oct through 31 Mar, and 1 Apr through 30 Sept.

2.5.4.2. Use the AMC AT/FP self-inspection checklist to report FP Performance Measure 2.A.12. Do not use the AMC IG Unit Compliance Checklist for this report, as it is a pared down version and may not incorporate the entire requirements of the AFI.

2.6. Installation/site commanders must appoint, in writing, a primary and alternate AT/FP Advisor. The primary AT Advisor will be assigned to a full time civil service position at wing XP Plans Division, identified under the installation commander's functional account code (FAC). The primary and alternate advisors serve as the Installation AT/FP subject matter experts. Installation alternate AT Advisors must be an officer or NCO (E-6 or above), designated by the Installation Commander. Recommend the alternate advisor be a Security Forces member. Those appointed as primary and alternate AT Advisors should not have secondary duties that conflict with or take precedence over, those duties associated with the AT program. Appointment of the AT Advisor shall be a primary duty. Individuals should have at least 18 months retainability, to serve in the installation AT position. Installation AT Advisors (primary and alternates) must receive Level II AT Training within 120 days of appointment. This requirement cannot be waived. The installation commander, based on mission need, may waive target grades for the alternate advisor; however, it must be done in writing. Once the primary and alternate Installation Advisors have been designated, forward a copy of the appointment letter containing the names, SSANs, security clearances, duty phone numbers and e-mail addresses to HQ AMC/SFOF. Update appointment letters as changes occur; pen and ink changes are not authorized.

2.6.1. All organizations on the installation, to include tenants and other DoD agencies, must appoint, in writing, a primary and alternate AT Advisor (must be an E-5 or above) to serve as the AT/FP subject matter expert and advisor, for the squadron, unit or agency. Once the primary and alternate AT Advisors have been designated, forward a courtesy copy of the appointment letter containing the names, SSANs, security clearances, duty phone numbers and e-mail addresses to the Installation AT Advisor. Update appointment letters as changes occur; pen and ink changes are not authorized.

2.6.2. TALCE deployments are not required to have an AT Level II trained individual, however, every effort should be made to ensure personnel are fully aware of AT/FP programs and requirements. If the TALCE is designated to stay in place as part of the follow-on force, an AT Level II trained individual should be assigned.

2.6.4. The primary Installation Advisor should be appointed, in writing, as the VAMP OPR. Provide a separate VAMP appointment letter to AMC/SFOF when changes occur. Do not combine the AT Advisor and VAMP letters.

2.7.2. All AMC installations are located in CONUS. The DIA is the only DoD agency authorized to determine the CONUS Terrorism Threat Level. AMC bases do not have the authority to set their own terrorism threat level. Commanders should consider the DIA threat level, along with the local threat assessment provided by the supporting OSI unit, to develop plans and programs to protect their assets. OSI units will provide current Local Threat Assessments (LTA) upon request. These LTAs, provide details regarding the current terrorism threat, the current DIA terrorism threat level, and any local situations of concern regarding possible threats to the military installations in the area.

2.7.2.1. (Added) Per Homeland Security Presidential Directive-3, March 11, 2002, the HSAS does not apply to military facilities. Installation AT Advisors and commanders should not use the Homeland Security (Terrorist Threat) Advisory System (HSAS) as a point of reference. The HSAS is designed to warn the public and private sector and uses different criteria to determine the advisory warning level. AMC installation commanders should not execute protection measures for their installation based on the HSAS. However, commanders may take action based on the intelligence information that drove the HSAS warning. Additionally, the DIA terrorism threat levels should not be confused or correlated with the Force Protection Conditions (FPCONs). Paragraph 2.7 strictly refers to the terrorism threat levels only, as defined in Attachment 4.

2.7.3. The AMC Threat Working Group (TWG) will, upon written or verbal request from OCONUS commanders who don't have AMC Intelligence personnel assigned, provide the most current terrorism threat in overseas areas of operation. Commanders should also refer to the HQ AMC Intelligence homepage for additional threat information. (<http://www.amcin.scott.af.smil.mil/homeIE.asp>)

2.7.4. (Added) Installation/site commanders should use intelligence information (to include terrorist, criminal and other potential threats, as well as the security environment of the local area) in developing/updating plans and programs to protect assets for which they are responsible.

2.8.4. Installation/Site Commanders shall task the appropriate intelligence/counterintelligence organizations under their command to collect, analyze, and disseminate terrorist threat information, as appropriate. Commanders at all levels shall ensure personnel under their command report information on events or situations that could pose a threat to the security of DoD personnel and resources.

2.8.4.1. (Added) To enlist the help of everyone at AMC installations and local communities, AFOSI created and manages the US Air Force Eagle Eyes program. The program puts each person on the anti-terrorism team by identifying the information needed to recognize and report suspicious behavior. This information can be submitted 24 hours a day and is immediately shared with the appropriate law enforcement agencies and military commanders for rapid assessment and investigation as necessary. Commanders should be familiar with the Eagle Eyes program and can contact the local AFOSI unit to obtain briefings and/or Eagle Eyes material (brochures, contact cards, etc.).

2.8.6. (Added) Although much of the information posted on the Internet is publicly available, intelligence professionals must follow established Intelligence Oversight (IO) guidelines regarding collection, storage, and dissemination of such Internet information.

2.8.7. (Added) Intelligence oversight (IO) also applies to vulnerability assessments (VAs). In the conduct of AT/FP awareness and VAs, the local threat assessment must come from the agency with the official mission to produce it (OSI for Air Force units). The VA team must use this as their threat baseline, and

cannot conduct their own threat assessment (primarily applies to CONUS threat assessments where the threat comes from domestic terrorists). IO applies to all AFSCs, not just intel. For example, Security Forces members must realize that when acting in an AT/FP or VA capacity, they are not engaged in law enforcement activity, and IO restrictions apply.

2.8.8. (Added) SECDEF policy guidance for Intelligence Support to Force Protection. Commanders and AT officers must be aware that military members are not to collect or disseminate information on U.S. persons, with very few exceptions. Some AT/FP officers are under the mistaken assumption that they can collect information on U.S. persons as long as the information is publicly available. THIS IS NOT TRUE. Publicly available information on U.S. persons can only be collected if such information is a specifically authorized function of an individual unit's mission. In general, this means CID, OSI and NCIS units. It does not mean AT/FP officers. Source: 181700ZNov98 Message, Subj: Policy Guidance for Intelligence Support to Force Protection.

2.8.9. (Added) The term "U.S. person" includes "U.S. citizens". It includes permanent resident aliens, unincorporated associations substantially composed of U.S. citizen or permanent resident aliens, and corporations incorporated in the U.S. and not directly controlled by a foreign government.

2.8.10. (Added) Intelligence oversight applies to all members of the DoD intelligence community, not just to collectors. DoD intelligence personnel engaged in any intelligence activity (e.g. collection, research, analysis, production, retention, or dissemination), as well as all non-intelligence personnel assigned to a DoD intelligence unit, must be familiar with the provisions of EO 12333, DoD Regulation 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons* and AFI 14-104, *Oversight of Intelligence Activities*.

2.10. Reports will be sent to HQ AMC/SFOF who will in turn pass the information to AFSFC/SFP.

2.10.1. Installation/site commanders shall task the appropriate intelligence/counterintelligence organizations under their command to collect, analyze, and disseminate terrorist threat information pertaining to the potential terrorist use of WMD.

2.11. The FPCON development process will incorporate the procedures outlined in paragraph [2.12.](#) as supplemented.

2.11.1. AMC/SFO is the executive agency for accomplishing FPCON messages for AMC/CC or AMC/CV release. All messages will be coordinated with the AMC FPWG/FPB prior to release, time permitting. All AMC generated FPCON messages to raise, lower, or initiate measures will be coordinated with the AMC Command Center (previously referred to as TACC/EA Cell) after coordination with AMC/CC or AMC/CV. After coordination with AMC Command Center, AMC/SF will transmit the message via DMS to the appropriate address group(s). AMC Command Center will also release an FPCON message to AMC command posts, IAW AFI 10-206, *Operational Reporting*, Table 3.1, rule 7b, Terrorist Events and attachment 3.

2.11.2.1. Installation commanders cannot lower higher-level directed FPCON measures without the higher-level commander's concurrence, IAW paragraph [2.13.2.1.](#) Installation commanders shall provide proposed measures for higher-level consideration, to the Director, Security Forces (AMC/SF) through DMS or official email. Provide a courtesy copy to the TACC Director of Operations (Senior Controller) through AMC Command Center, on all FPCON correspondence.

2.11.2.2. (Added) AMC SF Commanders will notify AMC/SF of any FPCON measures the installation is unable to fully implement. The memorandum will include corrective action, ECD for full implementation, and installation OPR.

2.11.3. (Added) AMC installations will utilize a standard FPCON sign system. These standards are meant to reduce visual clutter at facility entrances, provide a professional appearance, and quickly communicate the current FPCON condition. FPCON "NORMAL" signs will not be displayed. Only the AMC format shown at **Attachment 12 (Added) (Figure A12.1.** AMCVA 10-245, *Force Protection Condition A*, **Figure A12.2.** AMCVA 10-246, *Force Protection Condition B*, **Figure A12.3.** AMCVA 10-247, *Force Protection Condition C*, and **Figure A12.4.** AMCVA 10-248, *Force Protection Condition D*.) will be used. These Visual Aids are posted separately at <http://www.e-publishing.af.mil> and <http://www.amc.scott.af.mil/pubs/hqamc.htm>.

2.11.3.1. (Added) FPCON signs will be printed on colored paper or cardstock IAW their ISP and/or AT Plan.

2.11.3.2. (Added) Sign sizes may be either 4 ¼" x 5 ½" or 8 ½" x 11". The smaller format is preferred in most situations.

2.11.3.3. (Added) Signs will be laminated and mounded parallel with frame or mullion. Use minimal clear tape to affix the sign to the door in a location that is immediately visible at each entrance to the facility.

2.11.3.4. (Added) If laminated signs cannot be used at particular facility or entrance, recommend using clear acrylic document holders that won't detract from the appearance of the facility and that can be left empty when conditions are normal. The sign holder must be permanently mounted to either the door or wall in a location that is immediately visible upon entering the facility. Use an adhesive (clear silicon on glass doors) or screws to fasten the frame/holder to the door or wall. Avoid flexible sheet protectors or paper signs mounted directly with tape, as these do not present a proper professional image.

2.12. Develop local checklists from DoD O-2000.12-H, *Protection of DoD Personnel and Activities against Acts of Terrorism and Political Turbulence*. As a minimum, follow FPCON measures outlined in Attachment 3 of this supplement and the AFI. Commanders at all levels shall establish local measures to transition between FPCONs. These procedures will be included in installation AT plans.

2.12.1. Tenants on AMC bases should coordinate owning MAJCOM/Service directed FPCON changes with the host, and seek concurrence prior to implementation. Installation Commanders will consider the request, determine local threats, and make a base-wide determination. There should only be one FPCON on AMC bases with final determination by the installation/site commander.

2.12.3. (Added) After-action reports, containing comprehensive discussion of lessons learned will be forwarded to HQ AMC/SFOF within 30 days of a reported terrorist threat or terrorist incident.

2.13.2.1. Installation/Site Commanders may implement higher FPCONs based on local conditions. Downward directed FPCON changes for AMC units will come from or through AMC/CC. In those instances where local threats are absent, commanders will seek clarification from AMC prior to increasing FPCONs. There should only be one FPCON on AMC bases with final determination by the installation/site commander.

2.13.2.3. Installation commanders may implement higher FPCONs without prior notification if the threat warrants. Notify AMC Command Center as soon as possible after declaration of a higher FPCON, but not later than 12 hours after. Installation AT Advisors will notify AMC/SFOF via official email, within 3

hours of an Installation commander's determination to implement higher FPCONs and will include the AMC Command Center as an action addressee.

2.13.3. Document the semi-annual review and attach with the local FPCON measures. In the case of a FPWG, maintain minutes to provide review upon request.

2.13.4. Installations will develop and implement local Random Antiterrorism Measures (RAMs) encompassing all units from across the installation. RAMs will include all organizations on an installation to include (but not limited to) NAF functions, DECA, AAFES, local area schools on the installation, higher headquarter tenants. Installations with higher headquarter tenants will coordinate RAM employment with the Director of Staff (DS), or Executive Officer where the DS function does not exist.

2.13.4.2. Two of the three mandatory daily RAMs will be non-Security Forces related. RAMs will be employed during all FPCONs (including NORMAL) to enhance force protection. As a minimum, utilize the required RAMs contained in DoD 0-2000.12-H. Locally developed measures should be used, as directed by the installation/site commander. Base entry point checks (BEPCS) do not count as installation RAMs.

2.13.5. Installation commanders will develop local procedures, outlined in the installation AT plan.

2.14.2. AT/FP plans will be assessed during higher headquarters program reviews as identified in Standard 26 to DoDI 2000.16 and paragraph 3.26 in the AFI. Plans shall address areas outlined in DoD **Standard 2** as supplemented, and include these additional areas to meet security requirements (NOTE: this list is not all inclusive): media control during terrorist incidents, FPCON procedures, to include the means to rapidly advise all units of FPCON changes, and all DoD elements and personnel for whom the installation/activity has force protection responsibility. See paragraph **2.5.3.** for additional guidance.

2.14.2.1. (Added) AMC installations will establish a stand-alone AT plan. A copy of the installation AT plan will be forwarded to AMC/SFOF. For those installations that do not already have a stand-alone plan, they have 180 days from the date of this supplement to comply.

2.14.3. Installation AT Plans will also include:

2.14.3.7. (Added) Oversized Vehicle/Contract Vehicle Gate Operations.

2.14.3.8. (Added) Installation Entry Point Overwatch Procedures.

2.14.3.9. (Added) Guidance for conducting Local Vulnerability Assessments.

2.14.3.10. (Added) Team membership for conducting Local Vulnerability Assessments.

2.14.3.11. (Added) Employment of High-Tech screening devices i.e., ION Scanners/Sniffers, Vehicle X-Ray, Thermal Imagers, etc.

2.14.3.12. (Added) Local FPCON procedures, either attached to (CONFIDENTIAL) or as an Annex (FOUO).

2.14.3.13. (Added) Barrier Plan with numbers and priorities for employment. Physical drawings of placement for the barriers are required. The Barrier Plan must be coordinated with all base agencies, with emphasis on response force units to include: Fire Department, Medical Group, Security Forces and Alert Crews.

2.14.4. (Added) The installation force protection corporate structure, e.g., ISC, FPWG, will review all AT plans annually and when the local threat level changes. Installation AT Advisors will document and main-

tain all reviews of AT plans with the existing publication. Discrepancies should be corrected as soon as possible but before the next annual review.

2.14.5. (Added) All organizations on AMC installations will forward their specific AT/FP plans to the installation AT Advisor.

2.15. Installation OSI offices will forward a copy of their Terrorism Threat Assessment to AFOSI Region 3, no later than 30 days after completion or when changes occur.

2.15.4. Installation/Site Commanders shall ensure terrorist threat assessments for their area of responsibility are incorporated in the risk assessment development process and included in appropriate AT/FP plans.

2.16.1. AT plans must include tenant activities and/or DoD elements and personnel for whom the commander has force protection responsibility. Where there are multiple command authorities on the installation, the installation/site commander is responsible for coordinating the physical security plans for all units on the installation. Review these program plans on an annual basis or when the local threat level changes.

2.16.3. AMC installation commanders should not solely use pre-positioned temporary barriers as encouraged in the AFI since AMC/CV policy is to program for aesthetic, permanent barriers (refer to Force Protection Sustainment Team report, 4 Mar 2002). Examples include, benches, developed trees and shrubs, and high curbing on roadways. This also includes permanent, movable/removable barriers such as gates, drop arms and removable bollards. The intent is to eliminate jersey barriers wherever possible because of their appearance and temporary nature. The installation commander has discretion on how and where pre-positioned barriers will be employed.

2.16.3.1. (Added) The installation barrier plan will be an annex in the installation AT plan.

2.17.1. Close coordination must also be maintained with local authorities. Terrorist incidents may not be confined within the boundaries of the installation. Maintain appropriate MOA/MOUs that detail the response and containment efforts of incidents that are not confined to an installation.

2.17.1.1. Commanders of AMC tenant units will ensure procedures for the protection of AMC personnel are included in the host installation's terrorist incident response plan. Likewise, installation commanders will ensure procedures for protection of tenant organizations are included in their terrorist incident response plan.

2.17.2. The incident response plan will be coordinated with the Installation CE readiness flight via the installation Readiness Working Group. The plan will be exercised annually. Installation commanders should ensure coordination with off-base local response agencies are integrated into the exercise. When possible, a physical exercise is recommended over a "table-top" exercise. At no time, will there be two "table-top" exercises back-to-back.

2.17.3. Installation AT Advisors will establish a process to ensure all service and/or contractor personnel have adequate background checks before access is granted to the installation or vulnerable facilities. Determine installation vulnerable facilities using CARVER and/or D(M)SHARPP. The installation should correlate with the critical facility list in the AT Plan and/or ISP. The process to determine contractor access should be part of the AT Plan.

2.17.3.1. (Added) All installation contracts (wing generated) require an extensive force protection review. Installation commanders will establish procedures to ensure all contracts are reviewed for adequate force protection measures. See paragraph 2.5.2. for HQ AMC FPWG process as a model.

2.17.4. Installation entry procedures for non-base personnel attending base events should be included in the Installation Security Plan, IAW AFI 31-101, as supplemented. These procedures should be referenced in the AT Plan.

2.18. Terrorist consequence management preparedness and response measures will be included in the AT plan. Ensure the AT plan includes any necessary guidance and measures not addressed in other installation plans. Do not duplicate the consequence management portions of other installation plans such as the Full Spectrum Threat Response Plan 10-2, the Medical Contingency Response Plan, and the Civil Engineer Contingency Response Plan. However, where applicable, ensure the AT plan clearly and specifically references the relevant sections and paragraphs of other plans.

2.19.1. Local command authorities will exercise all portions of their AT plans annually. Exercises shall involve local off-base agencies to the extent possible, and encompass duty and non-duty hours. Exercises shall include all tenant activities and/or DoD elements and personnel for whom the commander has force protection responsibility. Properly documented "Real World" scenarios may satisfy portions of this requirement. Exercises should not be limited to raising and lowering FPCONs. Documentation should be maintained at the installation level; however, installation AT Advisor's will maintain documentation of all AT exercises for 2 calendar years.

2.19.1.4. It is the AT Advisors inherent responsibility to ensure the installation commander is aware of their role in exercise requirements.

2.20. AMC's review of installation AT programs and plans will be conducted during unit staff assistance visits (SAV). AMC CE, SC, SG, and SF directorates will conduct installation AT/FP reviews under their purview, during unit SAVs. AMC/SFO will conduct installation AT/FP reviews during security forces SAVs at an installation. All AMC reviews of installation AT/FP programs will be documented and maintained at the AMC/SFOF section.

2.20.1. AMC/SFO also conducts review of the installation AT program via the US TRANSCOM (USTC) Force Protection Oversight Program (FPOP) located on the SIPRNET. This database provides oversight with the standards contained herein. The updates to the FPOP are completed by AMC/SFOF semi-annually, utilizing an expanded Unit Compliance Checklist (UCI), received by each installation AT Advisor, 1 Apr & 1 Oct. Additional quarterly reporting to the database will be accomplished by AMC/SFOF without the use of checklist updates from the installation AT Advisor. Checklist completion is only required during the April and October reporting periods. AMC/CC monitors the FPOP as necessary, through the USTC FP directorate. Specific review of the AT Plan is not part of the FPOP.

2.21. Modification to the MILPDS program is not complete. As an interim measure, unit ancillary training managers will document (through any available method) the full name, rank, ssan, and date of training for each member receiving Level I training. This documentation will be kept on file for three years or two months after permanent change of station (PCS). Retention of the record beyond a member's PCS will provide Level I verification to a gaining commander, should the question arise. Refer to paragraph 2.22.4 for further documentation requirements.

2.21.2. (Added) Installation commanders will program funds for training courses such as Level II Installation AT Training, Dynamics of International Terrorism, Combating Terrorism on Military Installations,

and the Individual Terrorism Awareness Course. *NOTE*: Do not request funding quotas for Air Education and Training Command funded schools as these are not funded locally.

2.22.1. Commanders will develop written procedures to provide Level I training, conducted prior to overseas TDY or PCS. Family members, 14-years and older traveling beyond CONUS on official orders (not to include leaves) will receive Level I AT Awareness Training as part of their pre-departure requirements. Personnel who have not completed Level I Awareness training will not be issued orders for overseas travel. Gaining commanders may deny travel to personnel who do not accomplish AT Level I training. Every member should have access to the Joint Staff Guide 5260, available via <https://wwwmil.lackland.af.mil/afsf/> (click on Office, then locate HQ AFSFC, then select Force Protection Division, followed by Reference Library, and finally JCS Documents, for the JS Guide and other appropriate documents).

2.22.3.2. All DoD personnel assigned to an AMC installation, eligible for OCONUS deployment will receive Level I AT Awareness Training annually. All uniformed personnel attached to an AMC installation will receive Level I AT Awareness Training annually. For the purpose of providing training, AAFES and DECA personnel eligible to deploy OCONUS should be provided Level I training. Installation AT Advisors should make every attempt to ensure personnel not assigned under the installation commander, receives Level I training. Tenant organizations should comply with the host installation's Level I AT Awareness Training requirements. AT Advisors must document lack of cooperation in achieving installation-wide Level I training.

2.22.7. Installation commanders will report Air Force Strategic Plan, Vol. 2, Performance Plan FP Performance Measures 2.A.14, Implementation and Tracking of Level I Antiterrorism Training, semi-annually, no later than 1 Apr and 1 Oct of each year to AMC/SFOF. Installation commanders must coordinate on the report prior to release to AMC/SFOF. Installation AT Advisors should be afforded minimal levels of staffing in order for the Installation commander to provide coordination within the suspense dates above. Continue reporting during emergency conditions.

2.22.8.2. AMC installation commanders will not exempt individuals from Level II AT training requirements. Personnel within AMC who perform Level I AT Awareness Training will be trained at an approved MTT or school, as found in attachment 7. Installation AT Advisors must receive Level II AT Training within 120 days of appointment (see paragraph 6). This requirement cannot be waived.

2.23.3. Procedures will prohibit the issuance of orders for overseas travel (deployed, PCS, TDY or leave) for those personnel who have not received AT/FP training with special emphasis on AOR-specific threat and medical threats. Refer to attachment 5 for AOR specific web sites.

2.23.4. (Added) Mobility aircrews, accomplish annual AT training IAW AFI 10-245, *The Air Force Anti-terrorism(AT) Program Standards* and MDS specific AFI 11-2 series training instructions. Document this training as ARMS Event Code G110 (AT Level I Awareness Training).

2.23.5. (Added) AT training may be accomplished as part of the aircrew intelligence briefing. Prior to departing home station on missions outside the CONUS, crews will receive a briefing emphasizing terrorist, enemy, and friendly political and military developments in the area in which they will be operating. This briefing will also include AOR specific AT information as directed by the geographic CDR, OPOD, or OPLAN. Once in theater, aircrews should receive an intelligence update upon initial arrival at a forward operating location (FOL) or enroute stop, and thereafter as significant developments occur.

2.23.6. (Added) Aircrews and Phoenix Raven personnel who have received Level I AT/FP training in the past year, regularly deploying to OCONUS locations, retain an AT/FP training status similar to individu-

als deployed (TDY/PCS) continually to overseas locations. This training status remains in effect as long as they have traveled OCONUS within the past 6 months. Individuals who experience a break in travel of more than 6 months do not fall into this category, and are required to accomplish the required training prior to deployment.

2.23.7. (Added) AT awareness training is required for travel to Puerto Rico even though it is a US territory.

2.24. Individuals appointed as installation AT Advisors (primary and alternates) must attend Level II training within 120 days of appointment. Installation AT Advisors must be an E-6 or above. These personnel serve as advisors to the installation commander. Personnel appointed to this position should be in place at least one year. Installation commanders must appoint their AT Advisors in writing.

2.24.1. Installation AT Advisor will schedule Level II training through AMC/SFXT for their unit AT Advisors. Personnel selected to attend the Level II course must be prioritized as follows: (1) installation AT/FP Advisors (primary and alternate), (2) key personnel assigned to UTCs, and (3) other specialties on the installation key to successful UTC deployment, i.e., combat logistics, communications, prime beef, medical personnel and other unique teams. Submit prioritized Level II training requests to HQ AMC/SFXT through the Installation AT Advisor. Requests must include full name, rank/grade, SSN, security clearance, and duty phone to facilitate orders preparation. Each organization on the installation should have a primary and alternate AT Advisor, as part of the Installation AT Program.

2.24.2. AMC installations should use the Air Mobility Warfare Center (AMWC), Ft Dix, NJ for their Level II AT Training. Other training sites are available on a case-by-case basis. All requests for training should be through AMC/SFXT.

2.24.6.3. AMC units requiring training at other than Air Force courses of instruction must receive approval by AMC/SF prior to course selection. Individuals who are trained at other than Air Force courses of instructions should not serve as AT advisor to an Air Force installation commander, unless specific instruction encompasses Air Base vulnerability assessments. Squadron/unit advisors are encouraged to obtain Level II training from any available course of instruction. Individuals who will serve as Installation AT Advisors will attend an Air Force Level II course.

2.24.7. AMWC will report their monthly training numbers directly to HQ AFSFC/SFP and AMC/SFXT.

2.24.9.2. AMC Level III Pre-Command AT Training will be conducted by AMC/SF staff personnel in the grade of Lt Col or GS-12 and above. Exceptions to this rule are authorized if the person delivering the training has had previous command experience.

2.24.9.3. Installation Security Forces commanders are authorized to provide AT Level III training in the event there are squadron commanders who were unable to attend the MAJCOM Commanders Orientation Course prior to command. SF commanders must use the training requirements in Table 2.3 and the Joint Staff/DoD pre-approved Level III CD-ROM. Additionally, SF commanders must distribute the Antiterrorism/Force Protection Master Reference CD-ROM, that lists all the required publications commanders must have on hand. Installation AT Advisors must maintain copies of this CD-ROM.

2.24.10. U.S. TRANSCOM Force Protection (TCFP) receives quotas from the Joint Staff and allocates positions to AMC throughout the year. Installation AT Advisors should coordinate requests for available seminar slots through their Installation CC to AMC/SFOF. AMC/SFOF will conduct a cursory review of the duty position of the individual request, then forward the request to TCFP who will make final determination on allocation of seminar slots.

2.24.11. Installation commanders must have processes in place to ensure personnel assigned are not deployed or PCSed to a gaining commander without the proper level of AT training required herein. Failure to provide training must be corrected as soon as identified to alleviate reoccurrences.

2.25. In accordance with DoD Directive 2000.12, *DoD Antiterrorism (AT) Program*, and DOD 2000.12-H, *Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence*, installation commanders and AMC Staff Directors will conduct annual reviews of high-risk billets and identify all high-risk personnel assigned to their units/staff. When feasible, these personnel should attend a regional orientation course (Middle East Orientation Course, Latin America Orientation Course, etc.) at the United States Air Force Special Operations School, Hurlburt Field FL. Other available courses include the Individual Terrorism Awareness Course at the John F. Kennedy Special Warfare Center at Fort Bragg, North Carolina. Emergency response and medical incident command system officers are encouraged to attend terrorism response courses developed by the Department of Justice and Federal Emergency Management Agency (FEMA). AMC installation/site commanders deployed or deploying outside the continental United States will designate high-risk personnel based on localized threats at the deployed location.

2.25.2. All AMC general officers and senior executive schedule equivalents are designated “high-risk” personnel when assigned to high-risk/high-threat areas.

2.25.4. Executive officers, executive secretaries, and others responsible for accomplishing itineraries for general officers and DAF civilian equivalents are responsible for marking travel itineraries for official use only (FOUO) or classifying the itineraries confidential when required.

2.26.1.2. Vulnerability Classification Rules. A portion of the document where a vulnerability has been identified and it is associated with a specific U.S. military site identified in the same portion of the report is classified Confidential, at a minimum. A portion of the document where a vulnerability has been identified but is not associated with a specific U.S. military site identified in the same portion of the report is FOUO. When in doubt, the vulnerability should be classified.

2.26.2.1. Conducting a local VA demands a dedicated effort from all organizations and should be cohesive and jointly orchestrated. Daily cross-functional meetings enhance the assessment process. Commanders should release vulnerability assessment team members from their primary duties for the duration of the assessment. Normally, a local vulnerability should not take more than two weeks to complete. Installation commanders should be out-briefed upon conclusion of the assessment. Installation commanders shall validate and forward a copy of the local VA to their respective NAF and AMC/SFOF within 15 days of completion of the report. Local VA reports must be accomplished within 60 days of completion of the assessment.

2.26.2.1.1. Local VAs are not required to be conducted during the calendar year of a Higher Headquarters (HHQ) VA, however, there should be a period of no more than 15 months prior to, or preceding the HHQ VA. All local VAs must be documented and signed by the installation commander.

2.26.3. Installation commanders shall prioritize, track and report to their respective NAF commander, the action to be taken to address vulnerabilities identified in the VA. Refer to paragraph [2.26.13](#) for additional guidance on use of the VAMP. All local VAs must be inputted into the VAMP.

2.26.3.1. Installation commanders will contact AMC/SF if problems arise in receiving a HHQ VA within three years, as a minimum.

2.26.4. HQ AMC will conduct independent VAs of AMC installation/sites in addition to those conducted by the AF team and the JSIVA.

2.26.4.1. (Added) AMC VAT members may provide over-the-shoulder MAJCOM representation of all JSIVA or Air Force VAs. Prior coordination between the HHQ VA team leader and the FPWG representative is paramount, and required. Every effort should be made by AMC/SF to provide the over-the-shoulder representative, however any VAT member may assist.

2.26.4.2. (Added) Installation AT Advisors will coordinate all actions for HHQ VAs with AMC/SFOF.

2.26.5. HQ AMC/SF schedules JSIVA, AF and AMC vulnerability assessments of AMC installations and sites through HQ AF/XOFP. The schedule will be coordinated with the HQ AMC/IG Gatekeeper and the respective installation /site commander.

2.26.6. HHQ VAs take the place of the Local VA, however, no more than 15 months must pass between a HHQ and the next Local VA.

2.26.7. VAs will ensure installation/site commanders have included all tenant organizations (on the installation/site or remote but administratively attached), into force protection plans, and that they are afforded the same level of AT/FP support as AMC units.

2.26.8. Use the CARVER matrix and/or the D(M)SHARPP criteria when conducting criticality and vulnerability assessments. Descriptions on CARVER and D(M)SHARPP are at [Attachment 10 \(Added\)](#) and [Attachment 11 \(Added\)](#).

2.26.8.6.1. The AMC/VAT will assess local MOA/MOUs with local authorities, to include, but not limited to, Law Enforcement, Emergency Services, HAZMAT response, Fire and Medical Aid and joint use agreements. The assessment team will also review agreements to provide utility services (water, gas, electric) to the installation (to include off base Gov't housing areas).

2.26.8.6.4. (Added) The Installation AT Advisor must be familiar with all installation MOA/MOUs with local authorities, regarding response, containment, and recovery of a terrorist event, however, they are not necessarily the OPR for such agreements. The appropriate OPR shall maintain signed copies of any agreements pertaining to areas listed in paragraph [2.26.8.6.1](#).

2.26.8.6.5. (Added) As a minimum, assessments should include information from intelligence, logistics, medical, physical security, facility engineering, meteorological, explosive ordnance disposal, and NBC staff elements. The entire range of potential terrorist WMD should be considered when conducting assessments. Threats from commercial chemical, biological, nuclear, and radiological sources should be included as well as traditional military agents. Examples of factors to consider include: Individual protective clothing and equipment, collective protection equipment and facilities, medical response and emergency services capability, training of personnel, physical security and protective barriers, facility design and construction, early warning and detection, alarms and attack warning, threat intelligence, preventive medicine and vaccination programs, sustainment operations and follow on support, storage of bulk hazardous material, explosive ordnance disposal response capability/availability and food and water sources.

2.26.9. AMC VATs will consider off installation housing, utilities and other local military agencies when conducting the VA.

2.26.10. AMC VAT composition may vary based on the type of installation being assessed. The assessment team shall consist of a team chief (an O-6 appointed by the AMC FPB), assessment structural engineer, infrastructure engineer, communications/information management specialist, counterintelligence

specialist, antiterrorism/force protection and physical security specialists, preventive medicine specialist, and an operations readiness/response specialist. Other functional experts may augment the team as needed. Augmentation will depend on type of assessment required, the nature of the installation's/site's mission, the terrorist threat level, and the FPCON.

2.26.10.1. Installation commanders will ensure all requests for a Force Protection Integrated Support Team is routed to AMC/SF for further coordination to HQ AFSFC/SFP. Requests may be made to AMC/SF (Director or Deputy) in writing, via email or by phone, depending on the nature and severity (emergent need) of the request.

2.26.11. AT Advisors should also use the VAMP located on the SIPRNET for additional lessons learned and Best Practices. AT Advisors should make every effort to populate the VAMP with their own site specific best practices/lessons learned for appropriate cross-feed.

2.26.12. AMC/SFOF is the MAJCOM VAMP administrator. All installation requests for VAMP rights must be directed to AMC/SFOF, DSN 779-0647.

2.26.12.1. (Added) Installation AT Advisors must provide AMC/SFO with a letter listing their Installation VAMP administrators, within 30 days of a position or administrative change. The installation commander must sign the letter.

2.26.13. The AMC VA team should provide a final VA report on CD ROM within 60 days of the assessment visit to the Installation Commander. The commander should ensure the Installation AT Advisor receives the report in order to meet the 30-day requirement to populate VAMP.

2.26.14. The AMC VA team will use the Installation out-brief to identify, by color-coded scheme, the nine Critical Program Requirements listed in paragraph 2.26.15. The final report will also have reference to the nine Critical Program Requirements, as identified during the out-brief.

2.26.14.2. An actual return to an installation assessed as RED, may not be required if physical documentation is provided to the MAJCOM POC (i.e., AT Advisor appointment letter in writing or signed plans received by AMC).

2.26.16.6. Installation Commanders and Installation AT Advisor will have a VAMP account. Installation Vice Commanders and Mission Support Group Commanders may have a VAMP account.

2.26.16.7. (Added) NAF Commanders should maintain a VAMP account (monitored by AMC/SFOF) in order to review the installation VAMP program. NOTE: Paragraph 2.26.3.1. requires installation commanders to prioritize, track and report vulnerabilities to the next general officer following a VA. VAMP provides a means to accomplish this task via the NAF Commander's account.

2.26.17.1. (Added) Installation/Site Commanders must address, mitigate and correct AT/FP vulnerabilities identified during all vulnerability assessments, especially those that are procedural or relatively inexpensive and would improve the AT/FP posture. Conversely, high cost improvements must be considered in context with threat and risk assessment, and if necessary, planned for, and programmed.

2.26.17.2. (Added) Data entry into VAMP should initially be listed as "procedural", in order to timely input data into VAMP. Strict follow-up must be maintained to ensure the appropriate installation-level review (Threat Working Group, Force Protection Working Group and/or Installation Security Council) is conducted to address the vulnerabilities initially entered as "procedural". Project numbers, and funding information must be entered as soon as possible, following installation review.

2.26.17.3. (Added) The Installation VAMP administrator is not required to be the Installation AT Advisor.

2.27.1. The AMC Threat Working Group (TWG) will conduct pre-deployment assessments of contingency or forward operating locations, and ensure the most current terrorism, criminal, military and health threat information is available via the classified HQ AMC Intelligence homepage <<http://www.amcin.scott.af.smil.mil/homeIE.asp>>.

2.27.1.1. CENTCOM AOR specific vulnerability assessments can be found at the SIPRNET site: <http://recluse.centcom.smil.mil/ccjs/jsd.htm>. Personnel should also review the Joint Security Directorate (JSD) AT/FP Guide (unclassified), found on site.

2.28. Use AMCI 24-101, Vol 24, *AMC Passenger Terminal Force Protection* in addition to other applicable directives, when designing or upgrading air terminals.

2.28.2.3. Procedures for the AT/FP review must be in writing, in the installation supplement of this AFI.

2.29. These criteria must be used to determine if facilities/sites, either currently occupied or under consideration for occupancy by DoD personnel, can adequately protect occupants against terrorist attacks.

2.30.3. Where applicable, installation/site commanders will ensure residential security assessments for off-installation housing are conducted. Results of these evaluations, if conducted, must be documented and maintained on file for review by higher headquarters assessment officials pursuant to Standard 26.

2.30.8. (Added) AMC assigned forces located within or transiting geographical commander's AORs will comply with that commander's established requirements and guidance governing off-installation accommodations. This includes, but is not limited to, lodging, routes traveled and modes of travel.

2.31.3. Installation/site commanders shall consult with their servicing AFOSI detachment if executive protection/protective services are needed.

Chapter 3 (Added)

AMC AT AWARDS

3.1. (Added) . DoD AT/FP Recognition Program Awards. Each year, the Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (OASD SO/LIC) recognizes outstanding AT efforts and installation programs that clearly set precedence in the field of AT/FP.

3.1.1. (Added) . Units wishing to submit nomination packages for these awards must forward them through their Installation Commander or AMC Director (in the case of HQ AMC Squadron submissions) to HQ AMC/SFOF, no later than 28 February of the current calendar year. Address the package to HQ AMC/SFOF, 102 E. Martin St., Rm 230N, Scott AFB, IL 62225.

3.1.2. (Added) . Nomination packages should include details covering the previous calendar year. HQ AMC/SFOF will forward specific details and a notification message to AMC units each year.

3.1.3. (Added) . AMC/SFOF will establish a board process and select one AMC nominee for each category (as determined by OSD/SOLIC), to compete at Air Force level. AMC nominees will be formally recognized as MAJCOM AT/FP Award Winner for the specific category. Award winners should be recognized during the annual AMC Security Force's Conference. NOTE: Nominee's and packages can and should come from across the installation. This program is not exclusive to Security Forces.

A3.2. (Added) Measure 1A. Public Affairs will publish articles and other mass media publications to help educate and inform the base populace. Ensure procedures are in place to assure this same information reaches DoD families residing off the installation.

A3.2.1. (Added) Measure 1B. Ensure key personnel in all base WMD response agencies, including security, medical, bioenvironmental engineering, fire/HAZMAT, EOD, and CE readiness, are briefed on any chemical, biological, radiological, and explosive (CBRNE) threats.

A3.2.2. (Added) Measure 2A. This measure ensures unit readiness to immediately execute required actions through employment of core knowledge experts.

A3.2.2.1. (Added) Measure 2B. Because FPCON Alpha may be maintained indefinitely, on a quarterly basis, verify notification and recall procedures for key WMD crisis response and consequence management personnel, including the Disaster Control Group (DCG) and/or Survival Recovery Center (SRC) members, and specialized teams.

A3.2.2.2. (Added) Measure 3A. Monthly, owner/user will test the intrusion alarm and motion detection system at the base water-well field and reservoir, if alarmed. Consult with the security forces squadron for guidance on how to effectively conduct this test.

A3.2.2.3. (Added) Measure 4A. Vehicles entering the installation are only required to display DoD Form 2220 or produce locally approved vehicle passes. During this FPCON, randomly check identification (driver or one adult). In this FPCON, it is not intended for everyone in the vehicle to have their identification checked. Continue "hours of darkness" checks according to local procedures. Search 100% of all contract and oversized vehicles. Use of a Military Working Dog (MWD) and Ion Scanners to conduct searches of oversized vehicles are mandatory. If an installation has insufficient MWD assigned to perform this task, AMC/SF will be notified immediately. Ideally, the installation will create a stand-alone gate for oversized/contractor vehicles. The installation commander will define "oversized vehicle". Make every attempt to isolate this entry point away from the cantonment and aircraft parking areas. Search 100% of

all privately owned vehicles (those that have not met permanent or temporary registration requirements) at the time of their application for entry.

A3.2.2.4. (Added) Measure 5A. During Alpha, AMC Installations have been given sufficient manpower to employ additional security at the installation entry points, to enhance entry control procedures as part of antiterrorism procedures, contrary to “day to day” entry control. This “overwatch” position must be employed to enhance your first line of defense against a Vehicle Borne Improvised Explosive Device, VBIED. During this FPCON, the overwatch may assist with traffic control on a random basis.

A3.2.2.5. (Added) Measure 5B. In AMC, installations will employ a two-person security (RAM) patrol and focus efforts on early detection of potential threats at the installation entry points and perimeter. This patrol will be equipped with the latest force protection technological devices (Ion Scanners, hand-held magnetometers, portable tire busters) to aid with vehicle and personnel searches, as well as Night Vision Equipment. This patrol may be divided into two one-person patrols.

A3.2.2.6. (Added) Measure 5C. Isolate and control access to flightline aircraft parking areas, industrial aircraft maintenance facilities, runway and taxiways. Erect fencing and or barriers and establish a limited number of designated entry points IAW AMC standards and policy. In AMC, day-to-day operations at these entry points should be accomplished by Smart Card/Automated Entry Control/Key Pad type system. If the Installation Commander elects to position entry controllers fulltime or as a RAM, at these positions because automation is not utilized, owner/user will fulfill this requirement or sufficient READY personnel will be assigned to the Security Forces Squadron.

A3.2.2.7. (Added) Measure 5C.1. Where a facility makes up a portion of this perimeter, implement circulation control (e.g., cipher locks, automated entry systems, etc.). As a RAM, post owner/user personnel--check entry credentials, inspect hand carried and search POV's. Consult with your Flightline Constable for searching technique training.

A3.2.3. Measure 7.A. In AMC it's recommended that Installation Commanders conduct quarterly “table top” or “Command Post Exercises” to review these plans and checklist. It may also be necessary to convene the Installation Security Council and or Force Protection Working Group to review plans and checklist.

A3.2.7. (Added) Measure 10F. Because the actions of FPCON Alpha must be able to be maintained indefinitely, in AMC Commanders cannot exempt any of the measures under this FPCON without completion of an AF Form 116, Request for Deviation from Security Criteria.

A3.3. (Added) Measure 12A. Review WMD crisis response and consequence management plans, checklist and procedures. Command Post or Table Top Exercises are strongly encouraged.

A3.3.1. (Added) Measure 12B. CE Readiness and Bioenvironmental Engineering will place at least two NBC technicians on telephone standby.

A3.3.2. (Added) Measure 12C. Verify notification and recall procedures for installation crisis response, consequence management agencies and personnel, including the Disaster Control Group (DCG), Survival Recovery Center (SRC), Unit Control Centers (UCC) and specialized teams. Verify procedures by conducting actual (preferred) or simulated (personnel conduct notifications but do not physically report for duty) recalls.

A3.3.3. Measure 14. The creation of a 25-meter clear zone will complement the required inspections in Measure 16. After careful review of your facility listing, as compared to the threat in your region, it is generally not necessary to establish a 25 meter clear zone around every facility on the installation. There

is no Air Force or AMC requirement to cover facility identification signs or directional signs. Commanders must employ sound Risk Management when making these determinations.

A3.3.3.1. (Added) Measure 17A. Consider reducing delivery points to the absolute minimum. Centralized commercial deliveries should be restricted to one designated location for screening and distribution.

A3.3.4. Measure 19. The Office of Special Investigation is the office of primary responsibility for the portion of this Measure that discusses counter-surveillance.

A3.3.5. Measure 21. Consider town meetings and increased commander calls.

A3.3.6. Measure 22. In AMC this is interpreted as a check that's conducted at the base entry point/visitor control center at the time when visitors are requesting an AF Form 75. This search will include the vehicle as well. For Non-DoD ID cardholders requesting an AF 75, their vehicle will be searched during every entry (unless accompanied by the sponsor) to the installation if Charlie Measure 33 is in effect as a "plus measure" in Bravo. Utilize Magnetometers and hand held transfriskers to assist and enhance the searching of individuals.

A3.3.7. Measure 23. In AMC, each Installation will employ a two-person (RAM) patrol to assist other base patrols with this responsibility. Pay special attention to areas such as: Installation Entry Point searches, Commissary, BX, Food Courts, Day Care Centers, etc.

A3.3.8. Measure 24. Public Affairs and the OSI will initiate a campaign that routinely informs personnel and family members of the general situation and how they can participate in the "Eagle Eyes" Program.

A3.3.9. Measure 25. It may be prudent to establish a hardened barrier around certain critical/sensitive facilities to create standoff. Refer to your Installation Barrier Plan/Critical Facility listing. Facilities of a critical or sensitive nature are generally defined as single points of failure, C2, through C4, and facilities or equipment that if destroyed would result in mission failure.

A3.3.10. Measure 26. Personnel should also be briefed on the Rules of Engagement, communications/duress procedures, and emergency reporting procedures.

A3.3.10.1. (Added) Measure 28A. Review readiness of all tasked WMD response agencies, including first responders, specialized teams, DCG, SRC, and Unit Control Centers (UCC). Ready WMD/HAZMAT response equipment for immediate use.

A3.3.11. (Added) Measure 29A. In addition to the requirements in Measure 11, Installation entry control in this FPCON will also require a check of DoD or locally approved credentials, for at least one adult occupant. Commanders will also maintain an overwatch position as described in FPCON Alpha Measure 5A, however, personnel performing overwatch must not be involved with traffic control duties. The sentry is there to perform overwatch duties only. Should the Commander elect to employ an overwatch position as a final denial point during this FPCON, or because it's directed by HHQ to assume "plus" measures from higher FPCONS (measure 33-strict entry control), procedures must be IAW FPCON Charlie Measure 33A.

A3.3.12. (Added) Measure 29B. BEE, CEO, SFS, and OSI meet and recommend appropriate drinking water system "hardening" measures, (such as boosting system pressure and chlorination levels, and security measures at isolated storage tanks and pump houses) to the FPWG, DCG, SRC or TWG, after considering nature of threat, system mechanics/properties and operating costs. BEE recommends appropriate monitoring locations and schedule for free available chlorine and pH as an indicator for system contamination after conducting a threat/risk analysis.

A3.4. (Added) Measure 31A. Activate and staff the SRC or Contingency Support Staff (CSS) and UCCs. The SRC/CSS will have at least the following representatives: Security Forces, Fire Protection, EOD, CE Readiness, Medical and a Director. The SRC/CSS will assist the commander to implement passive defense measures and monitor Full Spectrum Threat Response preparedness through the UCCs. During periods of extended FPCON Charlie, the commander may release SRC/CSS members, if the installation has achieved (and can maintain) acceptable readiness levels.

A3.4.1. Measure 32. All installation “convenience” gates will be closed and barricaded.

A3.4.2. (Added) Measure 33A. In AMC, strictly enforce control of entry is defined as: At installation entry points control entry by use of the DD Form 2220 and proper DoD identification (at least one adult occupant). Visitors (between the “estimated” ages of sixteen to sixty-five) accompanying DoD employees must produce photo identification or obtain a visitors pass. Sponsors must report to the base entry point to escort visitors. Visitors will be searched IAW Measure 22, as supplemented. Also, during FPCON Charlie and Delta, or anytime this measure is implemented, active installation entry points will transition their gate “overwatch” position (as described in FPCON Alpha Measure 5A) to a final denial over-watch position. This position is the desired final denial point for incoming traffic. The position must have non-lethal means of denying unauthorized entry and must be positioned far enough away to have enough time to react to unauthorized vehicles (employing non-lethal means). Non-lethal includes but is not limited to, tire deflation devices, a blocking vehicles, or pop-up bollards. If the distance between the entry point and over-watch is limited because of existing road configurations, employ speed bumps, rumble strips, or serpentine between the gate and the over-watch to minimize speeds. Pre-established signals (between the entry controller and the over-watch position) must be in place to ensure the over-watch position clearly understands when a vehicle needs to be stopped and if lethal or non-lethal measures must be taken. If lethal force is employed as an option, a formal Operational Risk Management (ORM) review must be accomplished that addresses, at a minimum, rules of engagement, fields of fire, and potential fratricide. The installation commander must approve the ORM package.

A3.4.3. (Added) Measure 33B. Commanders should review their “key” or “critical” facility listing and after evaluating the regional threat, limit some, all, or none of the installation facilities (to include off-base assets) to a single point of entry and control with owner/user personnel or other positive entry control devices, (e.g., key control, card swipe or cipher locks). For DoD housing facilities implement plans to enhance security.

A3.4.4. (Added) Measure 33C. At flightline entry points, search all vehicles and positively identify all occupants. Emergency response vehicles may be exempted from search provided pre-established entry procedures have been established. It’s imperative the entry controller have immediate communication with a 24-hour dispatch center. Depending on the threat assessment for your region, it may be prudent to employ an armed (minimum of an M.16 rifle) over-watch guard at the flightline entry point(s). Create serpentine and employ portable tire busters at the over-watch position. Terminate visitor access to the flightline.

A3.4.4.1. (Added) Measure 33D. When intelligence indicates a potential for radiological attack, randomly screen vehicles for radioactivity during vehicle searches. Civil Engineer Readiness and Bioenvironmental Engineering flights possess radiological detection instruments (ADM 300 RADIACs) that can be used for this purpose. If these agencies cannot provide manpower to perform radiological screening, augmentees (not base entry controllers) may be trained to operate the detectors.

A3.4.5. Measure 34. In AMC this is defined as: Those facilities identified as “Critical” to mission accomplishment, especially single points of failure.

A3.4.6. (Added) Measure 35A. AMC/SG considers threat and advises on appropriateness of issuing pralidoxime chloride and atropine auto injectors to trained first responder personnel. MDG/CC’s determine auto injector distribution. Consider establishing temporary on-base lodging for key First Responder personnel (Civil Engineers, Medical, and Security Forces).

A3.4.6.1. (Added) Measure 35B. Activate a CBRNE Cell with BEE, CEX/CEF personnel trained to perform NBC and HAZMAT plotting and risk assessment (i.e., HPAC, VLS Track, CAMEO/ALOHA and ChemRAT), and serve as information officers for reconnaissance teams.

A3.4.7. Measure 36. Establish additional patrols, above and beyond those outlined in Measure 23. If the threat and intelligence warrants, during flight operations maintain continuous observation over approach and departure flight corridors. For installations where flight corridors are located in highly populated areas, coordinate with local authorities for assistance. In order to fulfill these requirements and many others, Security Forces will have their full complement of READY forces assigned in FPCON Charlie.

A3.4.8. Measure 38. All installation entry points will have “hardened” serpentine barriers between the gate and the over-watch position.

A3.4.9. Measure 40A. Rehearse all threat related emergency action procedures (e.g. building evacuations and disaster response). If not already completed in the previous FPCON, issue operational C2 canisters to Security Forces to include augmentees.

A3.4.10. Measure 40B. Civil Engineering should share messages with all first responder UCCs.

A3.4.11. (Added) Measure 40C. BEE recommends appropriate monitoring locations and schedule for free available chlorine and pH as an indicator for system contamination after conducting a threat/risk analysis in conjunction with CEO, SFS and OSI.

A3.5.12. Measure 51. Recall all off-duty security forces and establish temporary on-base lodging (e.g. base fitness center, hangar).

Attachment 9 (Added)

SAMPLE AT/FP BUDGET SUBMISSION FORMAT

MEMORANDUM FOR HQ AMC/SFOP

102 East Martin Street, Suite 110
Scott AFB, IL 62250-5318

FROM: (Unit)
(Street Address)
(City/Base, State, & ZIP Code)

SUBJECT: AT/FP Budget Submission

1. Point of contact information:

- a. AT Officer/NCO:
- b. Duty phone (DSN):
- c. E-mail address:

2. AT requirements:

a. Requirement One (Narrative)

- (1) Project/item name and project number (if applicable)
- (2) Description of the project, justification, and the AT vulnerability addressed
- (3) Cost
- (4) Special identifiers
 - (a) Project by Contract Management System project number and Facility Investment Metric rating (for Operations and Maintenance Real Property Maintenance by Contract projects only)
 - (b) Program Design Construction project number (for Military Construction facility projects only)
 - (c) Command, Control, Communications, and Computer Systems Requirement Document number (for communications and computer projects only)
 - (d) Document numbers (for "Memo Due Out" items only)

- (e) Will the item be purchased using the Government-Wide Purchase Card (GPC)?
 - (5) Ranking on the installation commander's priority list
 - (6) Impact if unfunded
- b. List additional requirements using the format above.

[Installation CC]

[Signature Block]

Attachment 10 (Added)

CARVER TARGET ANALYSIS TOOL

A10.1. (Added) The following is an explanation of the CARVER targeting process. US Special Operations Forces (SOF) uses this process in targeting adversary's installations. For that reason it is included as a tool to evaluate US installations from an adversarial point of view. For those familiar with the CARVER tool, it may be used in addition to or in lieu of other assessment processes.

A10.2. (Added) TARGET ANALYSIS PROCESS

A10.2.1. (Added) This attachment explains CARVER. CARVER is used to assess mission, validity, and requirements. It is also used in technical appreciation and target analysis. This attachment provides a step-by-step example of how to use CARVER.

A10.3. (Added) CRITICALITY, ACCESSIBILITY, RECUPERABILITY, VULNERABILITY, EFFECT, AND RECOGNIZABILITY FACTORS

A10.3.1. (Added) The CARVER selection factors assist in selecting the best targets or components to attack. As the factors are considered, they are given a numerical value. This value represents the desirability of attacking the target. The values are then placed in a decision matrix. After CARVER values for each target or component are assigned, the sum of the values indicate the highest value target or component to be attacked within the limits of the statement of requirements and commander's intent.

A10.4. (Added) CRITICALITY

A10.4.1. (Added) Criticality means target value. This is the primary consideration in targeting. A target is critical when its destruction or damage has a significant impact on military, political, or economic operations.

A10.4.2. (Added) Targets within a system must be considered in relation to other elements of the target system. The value of a target will change as the situation develops, requiring the use of time-sensitive methods respond to changing situations. For example, when one has few locomotives, railroad bridging may be less critical as targets; however, safeguarding bridges may be critical to maneuvering conventional forces that require use of such bridges. Criticality depends on several factors:

A10.4.2.1. (Added) Time: How rapidly will the impact of the target attack affect operations?

A10.4.2.2. (Added) Quality: What percentage of output, production, or service will be curtailed by target damage?

A10.4.2.3. (Added) Surrogates: What will be the effect on the output, production, and service?

A10.4.2.4. (Added) Relativity: How many targets are there? What are their positions? How is their relative value determined? What will be affected in the system or complex "stream"?

A10.4.3. (Added) **Table A10.1. (Added)** shows how criticality values are assigned on CARVER matrixes.

Table A10.1. (Added) Assigning Criticality Values.

<u>CRITERIA</u>	<u>SCALE</u>
Immediate halt in output, production, or service; target cannot function without it.	9-10
Halt within 1 day, or 66% curtailment in output, production, or service	7-8
Halt within 1 week, or 33% curtailment in output, production, or service	5-6
Halt within 10 days, or 10% curtailment in output, production, or service	3-4
No significant effect on output, production or service	1-2

A10.5. (Added) ACCESSIBILITY

A10.5.1. (Added) A target is accessible when an operational element can reach the target with sufficient personnel and equipment to accomplish its mission. A target can be accessible even if it requires the assistance of knowledgeable insiders. This assessment entails identifying and studying critical paths that the operational element must take to achieve its objectives, and measuring those things that aid or impede access. The adversary must not only be able to reach the target but must also remain there for an extended period. The four basic steps identifying accessibility are:

A10.5.1.1. (Added) Infiltration from the staging base to the target area.

A10.5.1.2. (Added) Movement from the point of entry to the target or objective.

A10.5.1.3. (Added) Movement to the target's critical element.

A10.5.1.4. (Added) Exfiltration.

A10.5.2. (Added) Factors considered when evaluating accessibility include, but are not limited to:

A10.5.2.1. (Added) Active and passive early warning systems.

A10.5.2.2. (Added) Swimmer detection devices.

A10.5.2.3. (Added) Air defense capabilities within the target area.

A10.5.2.4. (Added) Road and rail transportation systems.

A10.5.2.5. (Added) Type of terrain and its use.

A10.5.2.6. (Added) Concealment and cover.

A10.5.2.7. (Added) Population density.

A10.5.2.8. (Added) Other natural or synthetic obstacles and barriers.

A10.5.2.9. (Added) Current and climatic weather conditions.

A10.5.3. (Added) The analysis along each critical path to the target should measure the time it would take for the action element to bypass, neutralize, or penetrate barriers and obstacles along the way. Accessibility is measured in terms of relative ease or difficulty of movement for the operational element and the likelihood of detection. The use of standoff weapons should always be considered in such evaluations.

A10.5.4. (Added) **Table A10.2. (Added)** shows how accessibility values are assigned on CARVER matrices.

Table A10.2. (Added) Assigning Accessibility Values.

<u>CRITERIA</u>	<u>SCALE</u>
Easily accessible, standoff weapons can be employed	9-10
Inside a perimeter fence but outdoors	7-8
Inside a building but on ground floor	5-6
Inside a building but on second floor or in basement; climbing or lowering required	3-4
Not accessible or inaccessible without extreme difficulty	1-2

A10.6. (Added) RECUPERABILITY

A10.6.1. (Added) A target's recuperability is measured in time; that is, how long will it take to replace, repair, or bypass the destruction of or damage to the target? Recuperability varies with the sources and type of targeted components and the availability of spare parts availability. Factors which should be considered when assessing recuperability include, but are not limited to, the availability of:

A10.6.1.1. (Added) On-hand equipment such as railroad cranes, dry docks, and cannibalization.

A10.6.1.2. (Added) Restoration and substitution through redundancies.

A10.6.1.3. (Added) On hand spares.

A10.6.1.4. (Added) Equivalent OB equipment sets that backup critical equipment or components, and the effects of economic embargoes and labor unrest.

A10.6.2. (Added) **Table A10.3. (Added)** shows how recuperability values are assigned on CARVER matrices.

Table A10.3. (Added) Assigning Recuperability Values.

<u>CRITERIA</u>	<u>SCALE</u>
Replacement, repair, or substitution requires 1 month or more	9-10
Replacement, repair, or substitution requires 1 week to 1 month	7-8
Replacement, repair, or substitution requires 72 hours to 1 week	5-6
Replacement, repair, or substitution requires 24 to 72 hours	3-4
Same day replacement, repair, or substitution	1-2

A10.7. (Added) VULNERABILITY

A10.7.1. (Added) A target is vulnerable if the adversary has the means and expertise to successfully attack the target. When determining the vulnerability of a target, the scale of the critical component needs to be compared with the capability of the attacking element to destroy or damage it. In general, the attacking element may tend to:

A10.7.1.1. (Added) Choose special components.

A10.7.1.2. (Added) Do permanent damage.

A10.7.1.3. (Added) Prevent or inhibit cannibalization.

A10.7.1.4. (Added) Maximize effects through the use of onsite materials.

A10.7.1.5. (Added) Cause the target to self-destruct.

A10.7.2. (Added) Specifically, vulnerability depends on:

A10.7.2.1. (Added) The nature and construction of the target.

A10.7.2.2. (Added) The amount of damage required.

A10.7.2.3. (Added) The assets available; for example, personnel, expertise, motivation, weapons, explosives, and equipment.

A10.7.3. (Added) **Table A10.4. (Added)** shows how vulnerability values are assigned on CARVER matrices.

Table A10.4. (Added) Assigning Vulnerability Values.

<u>CRITERIA</u>	<u>SCALE</u>
Vulnerable to long-range laser target designation, small arms fire, or charges of 5 pounds or less	9-10
Vulnerable to light anti-armor weapons fire or charges of 5 to 10 pounds	7-8
Vulnerable to medium anti-armor weapons fire, bulk charges of 10 to 30 pounds, or very careful placement of smaller charges	5-6
Vulnerable to heavy anti-armor fire, bulk charges of 30 to 50 pounds, or requires special weapons	3-4
Invulnerable to all but the most extreme targeting measures	1-2

A10.8. (Added) EFFECT.

A10.8.1. (Added) The effect of a target attack is a measure of possible military, political, economic, psychological, and sociological impacts at the target and beyond. This is closely related to the measure of target criticality. The type and magnitude of given effects desired will help the adversary select targets and target components for attack. Effect in this context addresses all significant effects, whether desired or not, that may result once the selected target component is attacked. Traditionally, this element has addressed the effect on the local population, but now there are broader considerations. Effect is frequently neutral at the tactical adversarial level. For example, the primary effect of the destruction of two adjacent long-range radar sites in an early warning system may be to open a hole in the system that is of sufficient size and duration to permit our adversary to launch a successful attack against the installation. Effects can also include:

A10.8.1.1. (Added) The triggering of countermeasures.

A10.8.1.2. (Added) Support or negation of PSYOP themes.

A10.8.1.3. (Added) Unemployment.

A10.8.1.4. (Added) Reprisals against the civilian populace.

A10.8.1.5. (Added) Collateral damage to other targets.

A10.8.2. (Added) Possible effects can be speculative and should be labeled as such. Effects of the same attack may be quite different at the tactical, operational, and strategic levels. For example, the destruction of a substation may not affect local power supply but cuts off all power to an adjacent region.

A10.8.3. (Added) **Table A10.5. (Added)** shows how effect values are assigned on CARVER matrices.

Table A10.5. (Added) Assigning Effect Values.

CRITERIA	SCALE
Overwhelmingly positive effects; no significant negative effects	9-10
Moderately positive effects; few significant negative effects	7-8
No significant effects, neutral	5-6
Moderately negative effects, few significant positive effects	3-4
Overwhelmingly negative effects; no significant positive effects	1-2

A10.9. (Added) RECOGNIZABILITY

A10.9.1. (Added) A target's recognizability is the degree to which it can be recognized by the adversary and his intelligence collection and reconnaissance assets, under varying conditions. Weather has an obvious and significant impact on visibility. Rain, snow, and ground fog may obscure observation. Road segments with sparse vegetation and adjacent high ground provide excellent conditions for good observation. Distance, light, and season must also be considered. Other factors that influence recognizability include the size and complexity of the target, the existence of distinctive target signatures, the presence of masking or camouflage, and the technical sophistication and training of the adversary.

A10.9.2. (Added) **Table A10.6. (Added)** shows how recognizability values are assigned on CARVER matrixes.

Table A10.6. (Added) Assigning Recognizability Values.

CRITERIA	SCALE
The target is clearly recognizable under all conditions and from a distance; it requires little or no training for recognition	9-10
The target is easily recognizable at small-arms range and requires a small amount of training for recognition	7-8
The target is difficult to recognize at night in bad weather, or might be confused with other targets or target component; it requires some training for recognition	5-6
The target is difficult to recognize at night or in bad weather, even with small-arms range; it is easily confused with other targets or components, it requires extensive training for recognition	3-4
The target cannot be recognized under any conditions, except by experts	1-2

A10.10. (Added) CARVER MATRIX

A10.10.1. (Added) These CARVER factors and their assigned values are used to construct a CARVER matrix. For the adversary this is a tool for rating the desirability of potential targets and wisely allocating attack resources. For the installation commander, it is a tool to counter the adversary.

A10.10.2. (Added) To construct the matrix, list the adversary's potential targets in the left column. For strategic level analysis, list the installation's systems or subsystems (electric power supply, rail system). For tactical level analysis, list the complexes or components of the subsystems or complexes selected by your MEVA analysis. (**Table A10.7. (Added)** shows a sample matrix for a bulk electric power supply facility.)

A10.10.3. (Added) As each potential target is evaluated for each CARVER factor, enter the appropriate targets have been evaluated, add the values for each potential target. The sums represent the relative desirability of each potential target; this constitutes a prioritized list of targets. Attack those targets with the highest totals first.

A10.10.4. (Added) If additional men and/or munitions are available, allocate these resources to the remaining potential targets in descending numerical order. This allocation scheme will maximize the use of limited resources. Planners can use the CARVER matrix to present the installation's staff with a variety of adversary defeat options. With the matrix they can discuss the strengths and weaknesses of each COA against the installation's targeted facility.

Table A10.7. (Added) Complete CARVER Matrix.

An initial CARVER report and targeting folder that highlights gaps in the data may be prepared at this step. The folder is used to develop a detailed collection and reconnaissance and surveillance (R&S) plan

For Example: THE INSTALLATION'S BULK ELECTRIC POWER SUPPLY

POTENTIAL TARGETS	C	A	R	V	E	R	TOTAL
FUEL TANKS	8	9	3	8	5	6	41
FULE PUMPS	8	6	2	10	5	3	34
BOILERS	6	2	10	4	5	4	31
TURBINES	8	6	10	7	5	9	45
GENERATORS	4	6	10	7	5	9	41
CONDENSERS	8	8	5	2	5	4	34
FEED PUMPS	3	8	5	8	5	4	33
CIR. WATER PUMPS	3	8	5	8	5	4	33
GENERATOR STEP UP TRANSFORMER	10	10	10	9	5	9	53

Attachment 11 (Added)**DEMOGRAPHY/MISSION, SYMBOLISM, HISTORY, ACCESSIBILITY,
RECOGNIZABILITY, POPULATION, AND PROXIMITY (DSHARPP OR MSHARPP)
MATRIX EXPLANATION**

A11.1. (Added) The purpose of the D(M)SHARPP matrix is to analyze likely terrorist targets. Consideration is given to the local threat, likely means of attack available to the enemy, and variables affecting the disposition (e.g., “attractiveness” to enemy, potential psychological effect on community, etc.) of potential targets. This document provides an example of how to use D(M)SHARPP.

A11.1.1. (Added) After developing a list of potential targets, use the D(M)SHARPP selection factors to assist in further refining your assessment by determining the most likely (i.e., efficient, effective, and plausible) method of attack and identifying vulnerabilities to that type of attack. After the D(M)SHARPP values for each target or component are assigned, the sum of the values indicate the highest value target (for a particular mode of attack) within the limits of the enemy’s known capabilities.

A11.2. (Added) DEMOGRAPHY.

A11.2.1. (Added) Demography focuses mainly on the threat to personnel and asks the question “who are the targets?” Depending on the ideology of the terrorist group(s), being a member of a particular demographic group can make someone (or some group) a more likely target. Therefore, when assessing points in this area, determine whether or not the group(s) have a history of or are predicted to target:

A11.2.1.1. (Added) Military members.

A11.2.1.2. (Added) Family members (US citizens in general).

A11.2.1.3. (Added) Civilian employees of the US government (include local nationals).

A11.2.1.4. (Added) Senior officers or other high-risk personnel.

A11.2.2. (Added) Assess points to the target facility (scale of 1-5; 5 being worst) in this area based upon the MO of the group in targeting specific groups, and the potential for the target to be attacked based on its housing personnel of that particular group.

A11.2.3. (Added) Demography Criteria Scale:

A11.2.3.1. (Added) Facility routinely contains substantial numbers of personnel known to be targeted by the enemy.

A11.2.3.2. (Added) Contains known target group, but rarely in large concentrations.

A11.2.3.3. (Added) Little target value based on demographics of occupants.

A11.3. (Added) MISSION.

A11.3.1. (Added) Mission focuses mainly on the threat to the situations, activities, capabilities, and resources on an installation that are vulnerable to a terrorist attack. The mission components consist of the equipment, information, facilities, and/or operations or activities that are necessary to accomplish the installation’s mission. When assessing points in this area, determine whether or not an attack on mission components will cause degradation by assessing the components:

A11.3.1.1. (Added) Importance: Importance measures the value of the area or assets located in the area, considering their function, inherent nature, and monetary value.

A11.3.1.2. (Added) Effect: Effect measures the ramifications of a terrorist incident in the area, considering the psychological, economic, sociological, and military impacts.

A11.3.1.3. (Added) Recoverability: Recoverability measures the time required for the function occurring at that area to be restored, considering the availability of resources, parts, expertise and manpower, and redundancies.

A11.3.2. (Added) Assess points to the target equipment, information, facilities, and/or operations or activities (scale of 1-5; 5 being worst) in this area based upon the degree of mission degradation if attacked by a terrorist.

A11.3.3. (Added) Mission Criteria Scale:

A11.3.3.1. (Added) Installation cannot continue to carry out its mission until the attacked asset is restored.

A11.3.3.2. (Added) Ability to carry out a primary mission of the installation would be significantly impaired if this asset were successfully attacked.

A11.3.3.3. (Added) Half of the mission capability remains if the asset were successfully attacked.

A11.3.3.4. (Added) The installation could continue to carry out its mission if this asset were attacked, albeit with some degradation in effectiveness.

A11.3.3.5. (Added) Destroying or disrupting this asset would have no effect on the ability of the installation to accomplish its mission.

A11.4. (Added) SYMBOLISM.

A11.4.1. (Added) Assess whether the target represents, or is perceived by the enemy to represent, a symbol of a targeted group (e.g., symbolic of US military, Christianity, government, authority, etc.). Assess points in this area based upon the symbolic value of the target to the enemy.

A11.4.2. (Added) Symbolism Criteria Scale:

A11.4.2.1. (Added) High profile, direct symbol of target group or ideology.

A11.4.2.2. (Added) Low profile, direct symbol of target group or ideology.

A11.4.2.3. (Added) Low profile and/or obscure symbol of target group or ideology.

A11.4.2.4. (Added) (For MISSION) Asset is perceived to be vital to the mission of the installation.

A11.5. (Added) HISTORY.

A11.5.1. (Added) Do terrorist groups have a history of attacking this type of target? While you must consider terrorist trends worldwide, focus on local targeting history and capabilities.

A11.5.2. (Added) History Criteria Scale:

A11.5.2.1. (Added) Strong history of attacking this type of target.

A11.5.2.2. (Added) History of attacking this type of target, but none in the immediate past.

A11.5.2.3. (Added) Little to no history of attacking this type of target.

A11.6. (Added) ACCESSIBILITY.

A11.6.1. (Added) A target is accessible when an operational element can reach the target with sufficient personnel and equipment to accomplish its mission. A target can be accessible even if it requires the assistance of knowledgeable insiders. This assessment entails identifying and studying critical paths that the operational element must take to achieve its objectives, and measuring those things that aid or impede access. The enemy must not only be able to reach the target but must also remain there for an extended period. The four basic stages to consider, when assessing accessibility are:

A11.6.1.1. (Added) Infiltration from the staging base to the target area.

A11.6.1.2. (Added) Movement from the point of entry to the target or objective.

A11.6.1.3. (Added) Movement to the target's critical element.

A11.6.1.4. (Added) Exfiltration.

A11.6.2. (Added) Accessibility Criteria Scale:

A11.6.2.1. (Added) Easily accessible, standoff weapons can be employed.

A11.6.2.2. (Added) Inside Perimeter fence, climbing or lowering required.

A11.6.2.3. (Added) Not accessible or inaccessible without extreme difficulty.

A11.7. (Added) RECOGNIZABILITY.

A11.7.1. (Added) A target's recognizability is the degree to which an operational element and/or intelligence collection and reconnaissance asset under varying conditions can recognize it. Weather has an obvious and significant impact on visibility (yours and the enemy's). Rain, snow, and ground fog may obscure observation. Road segments with sparse vegetation and adjacent high ground provide excellent conditions for good observation. Distance, light, and season must be considered.

A11.7.2. (Added) Other factors that influence recognizability include the size and complexity of the target, the existence of distinctive target signatures, the presence of masking or camouflage, and the technical sophistication and training of the enemy.

A11.7.3. (Added) Recognizability Criteria Scale:

A11.7.3.1. (Added) Target is clearly recognizable under all conditions and from a distance; requires little or no training for recognition.

A11.7.3.2. (Added) Target is easily recognizable at small-arms range and requires a small amount of training for recognition.

A11.7.3.3. (Added) Target is difficult to recognize at night or in bad weather, or might be confused with other targets; requires training for recognition.

A11.7.3.4. (Added) Target cannot be recognized under any conditions—except by experts.

A11.8. (Added) POPULATION.

A11.8.1. (Added) What is the population relative to other potential targets? Going on the assumption the intent of the attack is to kill or injure personnel, it follows that the more densely populated an area/facility is, the more lucrative a target it makes (all other things being equal).

A11.8.2. (Added) Population Criteria Scale:

A11.8.2.1. (Added) Densely populated; prone to frequent crowds.

A11.8.2.2. (Added) Relatively large numbers of people, but not in close proximity (i.e., spread out and hard to reach in a single attack).

A11.8.2.3. (Added) Sparsely populated; prone to having small groups or individuals.

A11.8.2.4. (Added) (For MISSION) The population is comprised of personnel deemed vital to the accomplishment of the installation's mission.

A11.8.2.5. (Added) (For MISSION) Population has no special segment necessary for mission accomplishment.

A11.8.2.6. (Added) (For MISSION) Sparsely populated or unattended.

A11.9. (Added) PROXIMITY.

A11.9.1. (Added) Is the potential target located near other personnel, facilities, or resources that, because of their intrinsic value or "protected" status and a fear of collateral damage, afford it some form of protection? (i.e., near national monuments, protected/religious symbols, etc., which the enemy holds in high regard). *NOTE:* It is important to consider whether the target is in close proximity to other likely targets. Just as the risk of unwanted collateral damage may decrease the chances of attack; a "target-rich" environment may increase the chances of attack.

A11.9.2. (Added) Proximity Criteria Scale:

A11.9.2.1. (Added) Target is isolated; no chance of unwanted collateral damage to protected symbols or personnel.

A11.9.2.2. (Added) Target is in close enough proximity to place protected personnel, facilities, etc., at risk of injury or damage, but not destruction.

A11.9.2.3. (Added) Target is in close proximity; serious injury/ damage or death/total destruction of protected personnel/facilities likely.

A11.9.3. (Added) **Table A11.1. (Added)** is an example DSHARPP worksheet. **Table A11.2. (Added)** is an example MSHARPP worksheet. Values from 1 to 5 are assigned to each factor based on the associated data for each target. Five represents the highest vulnerability or likelihood of attack and 1 the lowest. Accordingly, the higher the total score, the more vulnerable the target. Because this analysis is highly subjective, some analysts prefer simple "stoplight" charts with red, yellow and green markers representing descending degrees of vulnerability. The D(M)SHARPP analysis must consider both the present force protection posture and enhanced postures proposed for escalating FPCONs.

Table A11.1. (Added) DSHARPP Worksheet.

TARGET	D	S	H	A	R	P	P	TOTAL	WEAPON
Barracks A	4	4	5	1	3	3	1	21	4,000 Truck IED
Barracks B	4	4	5	4	2	5	4	28	4,000 Truck IED
HQ BLDG	5	5	4	1	4	3	2	24	50 lb Satchel Charge
Pax Term	3	3	3	2	3	1	5	20	220 lb Car IED
PX	2	2	1	3	4	2	3	17	4,000 lb Truck IED
Family Housing	1	1	2	5	1	4	1	15	220 Car IED
Parade Ground	5	2	4	5	5	5	3	29	Small unit Raid

Table A11.2. (Added) MSHARPP Worksheet.

TARGET	M	S	H	A	R	P	P	TOTAL	WEAPON
HQ BLDG	3	4	5	1	3	3	1	20	4,000 Truck IED
Barracks B	3	4	5	4	4	4	2	26	220 lb Car IED
Comm Center	5	4	2	3	5	3	1	23	4,000 Truck IED
SF Ops Center	3	3	2	4	4	4	2	22	7.62 (Sniper)
Fuel Storage	4	3	1	5	5	1	3	22	50 lb Satchel Charge
Hanger A	5	5	3	2	5	5	4	29	Mortar
Wpns Storage	5	5	1	1	5	3	1	21	RPG
Bec Transformer	5	2	3	5	5	1	4	25	Grenade

A11.9.4. (Added) Specific target vulnerabilities must be combined with exploitable perimeter control vulnerabilities. If access routes are well protected and not deemed exploitable an otherwise vulnerable building becomes a less likely target.

Attachment 12 (Added)

FORCE PROTECTION CONDITIONS

Figure A12.1. AMCVA 10-245 Force Protection Condition A.

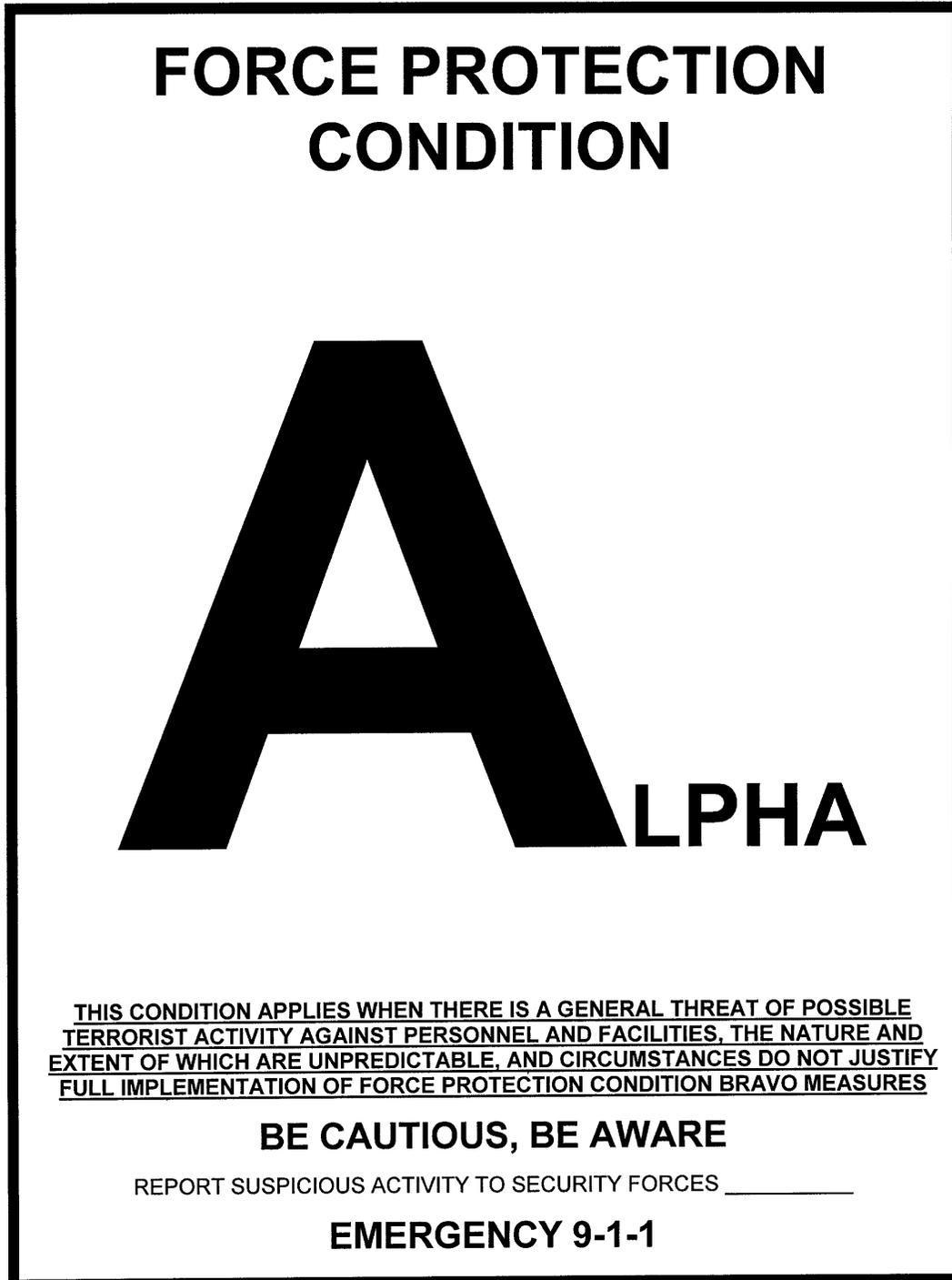


Figure A12.2. AMCVA 10-246 Force Protection Condition B.

**FORCE PROTECTION
CONDITION**

B

RAVO

THIS CONDITION APPLIES WHEN AN INCREASED AND MORE PREDICTABLE
THREAT OF TERRORIST ACTIVITY EXISTS

BE CAUTIOUS, BE AWARE

REPORT SUSPICIOUS ACTIVITY TO SECURITY FORCES _____

EMERGENCY 9-1-1

Figure A12.3. AMCVA 10-247 Force Protection Condition C.

**FORCE PROTECTION
CONDITION**

C

HARLIE

THIS CONDITION APPLIES WHEN AN INCIDENT OCCURS OR INTELLIGENCE IS
RECEIVED INDICATING SOME FORM OF TERRORIST ACTION AGAINST PERSONNEL
OR FACILITIES IS IMMINENT

BE CAUTIOUS, BE AWARE

REPORT SUSPICIOUS ACTIVITY TO SECURITY FORCES _____

EMERGENCY 9-1-1

Table A12.4. AMCVA 10-248 Force Protection Condition D.

**FORCE PROTECTION
CONDITION**

D

ELTA

THIS CONDITION APPLIES IN THE IMMEDIATE AREA WHERE A TERRORIST ATTACK
HAS OCCURRED OR WHEN INTELLIGENCE HAS BEEN RECEIVED THAT TERRORIST
ACTION AGAINST A SPECIFIC LOCATION OR PERSON IS LIKELY

BE CAUTIOUS, BE AWARE

REPORT SUSPICIOUS ACTIVITY TO SECURITY FORCES _____

EMERGENCY 9-1-1

JAMES R. HUTCHISON, Colonel, USAF
Director of Security Forces