Unclassified/FOUO

Joint Publication 3-07.2

Joint Tactics, Techniques, and Procedures for Antiterrorism

Second Draft
8 December 2004

Unclassified/FOUO

PREFACE

1. Scope

~~This publication sets forth the tactics, techniques, and procedures governing the joint conduct of United States (US) antiterrorism (AT) operations. It provides a basis for understanding US national policy and general objectives relating to antiterrorism and explains important Department of Defense (DOD) and US Government agency command and control relationships. In addition, it outlines basic US military antiterrorism capabilities and provides commanders with guidance on how to organize, plan, and train for the employment of US forces in interagency and multinational antiterrorism operations.~~

This publication provides guidance and sets forth tactics, techniques, and procedures on how to organize, plan, and train for the joint employment of United States (US) forces in joint antiterrorism (AT) operations. It outlines US national policy and objectives relating to AT, explains important Department of Defense (DOD) and US government agency command and control relationships, and basic US military AT capabilities.

2. Purpose

This publication has been prepared under the direction of the Chairman of the Joint Chiefs of Staff ~~(CJCS)~~. It sets forth joint tactics, techniques, and procedures (JTTP) to govern the joint activities and performance of the Armed Forces of the United States in joint operations and provides the doctrinal basis for interagency coordination and US military involvement in multinational ~~and interagency~~ operations. It provides military guidance for the exercise of authority by combatant commanders and other joint force commanders (JFCs) and provides military guidance for use by the Armed Forces in preparing their appropriate plans. It is not the intent of this publication to restrict the authority of the joint force commander from organizing the force and executing the mission in a manner the JFC deems most appropriate to ensure unity of effort in the accomplishment of the overall mission.

3. Application

a. The JTTP and guidance established in this publication apply to the commanders of combatant commands, subunified commands, joint task forces, and subordinate components of these commands. These principles and guidance also may apply when significant forces of one Service are attached to forces of another Service or when significant forces of one Service support forces of another Service.

b. The guidance in this publication is authoritative; as such, these JTTP will be followed except when, in the judgment of the commander, exceptional circumstances dictate otherwise. If conflicts arise between the contents of this publication and the contents of Service publications, this publication will take precedence for the activities of joint forces unless the Chairman of the Joint Chiefs of Staff, normally in coordination with the other members of the Joint Chiefs of Staff, has provided more current and

specific guidance. Commanders of forces operating as part of a multinational (alliance or coalition) military command should follow multinational doctrine and procedures ratified by the United States. For doctrine and procedures not ratified by the United States, commanders should evaluate and follow the multinational command's doctrine and procedures, where applicable and consistent with US law, regulations, and doctrine.

TABLE OF CONTENTS

PAGE

EXECUTIVE SUMMARY ..... TBD

CHAPTER I
INTRODUCTION

- General I-1
- Purpose I-1
- Force Protection and Antiterrorism Relationship ..... I-~~3~~2
- Overview of Antiterrorism Program Elements ..... I-~~3~~4
- Overview of Department of Defense Role and Responsibility ..... I-~~4~~

CHAPTER II
TERRORIST THREAT

- General II-1
- ~~Underlying Conditions~~Terrorist Tactics II-1
- ~~Operating Environment~~Terrorist Groups II-6
- Terrorist Organization ~~Modern Technologies~~ II-7
~~Tactics~~
- ~~Terrorist Group Structure and Organization~~ Terrorism Against the Homeland II-13
~~Targets~~
~~Domestic Terrorism~~

CHAPTER III
INTELLIGENCE, COUNTERINTELLIGENCE, AND THREAT ANALYSIS

- Intelligence and Counterintelligence III-1
- Threat ~~Assessment~~Analysis ..... III-~~16~~10
- Countersurveillance..... III-12

CHAPTER IV
LEGAL CONSIDERATIONS

- Authority ..... IV-~~6~~1
- Limits of Military and Intelligence Support to Civil Authorities ..... IV-~~7~~2
- ~~Jurisdiction and Authority for Handling Terrorist Incidents ..... IV-18~~
- Federal Agencies and the Military ..... IV-~~23~~7
- Military Installation Commander's Responsibilities ..... IV-~~43~~20

CHAPTER V
ANTITERRORISM PROGRAM; INSTALLATION, BASE, SHIP, UNIT, AND PORT

- Overview of Program Concept V-1
- Antiterrorism Plan Development ..... V-~~24~~8
- Combatant Commander's Responsibility ..... V-~~32~~9

CHAPTER VI
PREVENTIVE MEASURES AND CONSIDERATIONS

- Commander's Responsibility VI-1
- Antiterrorism Force Protection in High-Threat Areas VI-1
- Tactical Force Protection ..... VI-~~22~~14
- Suicide Bombers/High Risk Vehicle Checkpoints..... VI-14

CHAPTER VII
TERRORIST INCIDENT RESPONSE AND TERRORISM CONSEQUENCE MANAGEMENT

- General VII-1
- Terrorist Incident Management Planning ..... VII-~~3~~2
- Initial Response ..... VII-~~4~~2
- Follow-On Response ..... VII-~~10~~4
- Initial Response to a ~~Weapons of Mass Destruction Attack~~CBRNE Atack ..... VII-~~15~~5
- Special Considerations ..... VII-~~18~~7

APPENDICES

A Threat Assessment A-1
B Vulnerability Assessment B-1
C Criticality Assessment C-1
D Sample Antiterrorism Plan Format D-1
E Antiterrorism Checklist E-1
F Force Protection Condition System F-1
G Maritime Security Conditions G-1
H High Risk Personnel Protection H-1
J Jurisdictional Authority for Handling Terrorist Incidents J-1
K References K-1
L Administrative Instructions L-1

GLOSSARY

Part I Abbreviations and Acronyms GL-1
Part II Terms and Definitions GL-8

FIGURES

I-1 Antiterrorism & Counterterrorism I-2
I-2 Force Protection I-3
II-1 Categories of Terrorist Groups ..... II-~~13~~7
II-2 ~~Terrorist Organization Basic~~ Structure Pyramid of a Typical Terrorist Organization ..... II-~~19~~8
III-1 Sources of Intelligence and Counterintelligence ..... III-~~3~~2
III-2 Information Requirements ..... III-~~16~~9
IV-1 Request for Assistance ..... IV-~~9~~3
~~IV-2 Federal Territorial Jurisdiction Categories ..... IV-19~~
IV-~~3~~2 Approval for Use of Military Force ..... IV-~~42~~19
VI-1 Situation Estimate Checklist..... VI-3
VI-~~1~~2 Security Force Equipment ..... VI-~~8~~6
VI-~~2~~3 Principles of Riot Control ..... VI-~~21~~13
VII-1 Special Considerations ..... VII-~~23~~9
J-1 Jurisdictional Authority for Handling Terrorist Incidents J-1

CHAPTER I
INTRODUCTION

"There is another type of warfare — new in its intensity, ancient in its origin — war by guerrillas, subversives, insurgents, assassins; war by ambush instead of by combat, by infiltration instead of aggression, seeking victory by eroding and exhausting the enemy instead of engaging him . . . It preys on unrest . . . "

John F Kennedy
Address to the Graduating Class,
US Naval Academy, 6 June 1962

1. General

The term "terrorism" is defined as the calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological (Joint Publication (JP) 1-02). This definition is the foundation, throughout this publication, for the guidance to ~~combatant commanders, subunified commanders, joint task force (JTF) commanders, and component~~ joint force commanders (JFCs) and their subordinates. Specific policy, directive guidance, standards, and procedures for the Department of Defense (DOD) ~~combating~~ antiterrorism (AT) ~~terrorism (CbT)~~ program is contained in DOD Directive (DODD) 2000.12, "*D~~o~~OD Antiterrorism (AT) Program*," August 18, 2003, ~~DOD Instruction (DODI) 2000.14, *DoD Combating Terrorism Program Procedures,*~~ DOD~~D~~ O-2000.12-H, "*D~~o~~OD Antiterrorism Handbook,*" *9 February 2004,* and D~~o~~oDI O 2000.16, *D~~o~~OD Antiterrorism Standards*" (DRAFT), March XX, 2004.

2. Purpose

Combating terrorism involves actions including antiterrorism (AT) (defensive measures used to reduce the vulnerability to terrorist acts), ~~and~~ counterterrorism (CT) (offensive measures taken to prevent, deter, preempt and respond to terrorism), terrorist consequence management (preparation for and response to consequences of a terrorist incident), and intelligence support (collection or dissemination of terrorism related information), taken to oppose terrorism throughout the entire threat spectrum. This publication ~~addresses only AT~~ does not address CT. The following definitions, also shown in Figure I-1, are provided to assist in understanding the difference between AT and CT:

a. Antiterrorism is defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military and civilian forces.

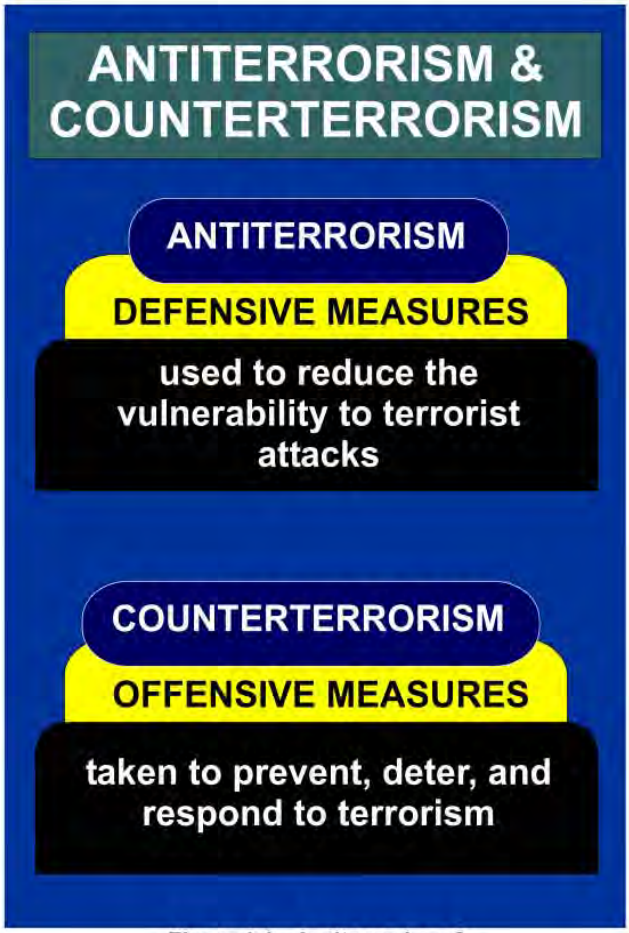

Figure I-1. Antiterrorism & Counterterrorism

b.Counterterrorism is offensive measures taken to prevent, deter, and respond to terrorism. Sensitive and compartmented CT programs are addressed in relevant National Security Decision Directives, National Security Directives, ~~contingency~~ joint operation plans, and other relevant classified documents.

3. Force Protection and Antiterrorism Relationship

a. Force protection (FP) should not be used as a synonymous term with AT or other supporting tasks. It is an overarching concept and mission responsibility inherent to command within all military operations. As discussed throughout this publication, AT, in contrast, is a sub-element of combating terrorism, which is a subset of the broader FP concept.

(1) Force protection: The DOD approved definition of FP is currently articulated as: "Actions taken to prevent or mitigate hostile actions against DOD personnel (to include

family members), resources, facilities, and critical information. FP does not include actions to defeat the enemy or protect against accidents, weather, or disease." These actions conserve the force's fighting capability so it can be applied at the decisive time and place and incorporate the coordinated and synchronized offensive and defensive measures to enable the effective employment of the joint force while degrading the opportunities of the enemy.

(2) Antiterrorism: AT, on the other hand, is described as: "Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military and civilian forces." While AT integrates other defensive actions (such as physical security, CBRN defense, operations security, counterintelligence, construction standards, etc,) in a comprehensive program designed to protect against terrorist attack, it does not include all the aspects of FP.

(3) FP is a joint task. As such, joint force commanders conduct FP in similar fashion as movement and maneuver; intelligence, surveillance, and reconnaissance; employing firepower; sustaining operations; operating in a CBRN environment; and providing command and control during the execution of campaigns, major operations, and tactical engagements. FP actions are to be accomplished by the Services and by joint forces under

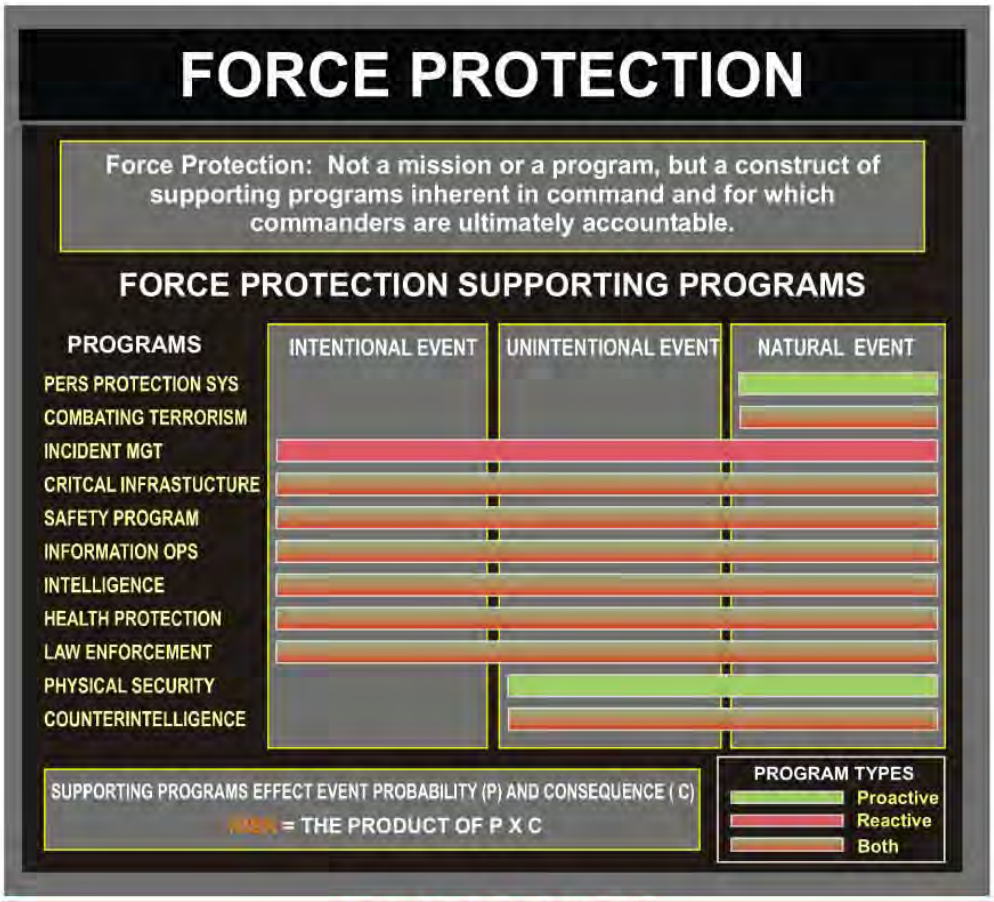

Figure I-2. Force Protection

joint command and control using joint doctrine. FP can be applied at multiple levels of command, from the strategic-theater, through the operational, and down to the tactical level.

4. Overview of ~~AT~~ Antiterrorism Program Elements

The ~~Department of Defense's~~ DOD's AT program is one of several security-related programs that fall under the overarching FT concept. ~~Combating Terrorism and Force Protection programs.~~ The AT program ~~shall be~~ is a collective, proactive effort focused on the ~~prevention and detection~~ detection and prevention of terrorist attacks against DOD personnel, their families, facilities, installations, and infrastructure critical to mission accomplishment as well as the preparations to defend against and planning for the response to the consequences of terrorist incidents. Although not elements of AT, plans for terrorism consequence management preparedness and response measures as well as plans for continuing essential military operations are important adjuncts to an effective AT program. ~~The minimum elements of an AT program shall be all the elements and assessments of the risk management process, planning, training and exercises, resource generation, and program reviews~~. The minimum elements of an AT program are: risk management, planning, training and exercises, resource generation, and comprehensive program review. The process, or sequence, of AT program elements should be iterative and serve continuously to refine the AT ~~P~~plan.

Every commander has ~~a~~ the responsibility for the security of the command against ~~varying levels and types of~~ terrorist ~~threat~~ attacks.

5. Overview of DOD Role and Responsibility

a. ~~It is~~ DOD policy ~~that:~~

(1) ~~The~~ DOD ~~C~~components ~~and the DOD~~ elements, and personnel shall be afforded ~~protected~~ protection from terrorist acts through a ~~high priority,~~ comprehensive AT program. ~~The Department of Defense's AT program shall be all encompassing using an integrated systems approach.~~ The DOD's AT program shall be one of the programs, when executed, that contributes to the commander's overall FP responsibility.

(2) The ~~C~~commanders at all levels have the responsibility and authority to enforce appropriate security measures to ensure the protection of DOD elements and personnel subject to their control. Commanders ~~and~~ shall ensure the AT awareness and readiness of all DOD elements and personnel (including dependent family members) assigned or attached. ~~Commanders~~ They must also ensure appropriate AT protection and readiness of DOD elements and personnel while pursuing mission accomplishment.

(3) The geographic ~~C~~combatant ~~C~~commanders' AT policies take precedence over all AT policies or programs of any DOD ~~C~~component operating or existing in that command's area of responsibility (AOR) except for those under the security responsibility of a ~~C~~chief of ~~M~~mission (COM). All DOD personnel traveling into a ~~C~~combatant ~~C~~commander's AOR will familiarize themselves with all AOR-specific AT policies and comply with them.

(4) A Combating Terrorism Readiness Initiatives Fund (CbT-RIF) is maintained to provide a flexible means to respond to emergent and/or emergency AT requirements (Chairman of the Joint Chiefs of Staff Instruction 5261.01~~B~~C). More information can be found online at "www.atep.smll.mil."

(5) All DOD military, DOD civilians, DOD dependent family members, and DOD contractors shall comply with theater, country, and special clearance requirements (DOD Directive 4500.54,*Official Temporary Duty Travel Abroad*, and D~~o~~OD 4500.54-G, *D~~o~~OD Foreign Clearance Guide (FCG)*, before overseas travel).

(6) Commanders do not have the same legal responsibility to provide security for DOD contractors as that provided for military forces or direct-hire employees. Contractors remain private US citizens. The Department of Defense shall assist the Department of State (DOS), where militarily feasible, in supporting efforts to protect US citizens abroad. Contractors are required to contact the ~~C~~combatant ~~C~~command to obtain, and comply with, the specific AT guidance for that particular area. Commanders are required to offer AT training to contractors under the terms specified in the contract. Contractors working within a US military facility or in close proximity of US Forces shall receive incidentally the benefits of measures undertaken to protect US Forces. Additionally, commanders may provide an additional, higher level of security, to which the government may have agreed pursuant to a particular contract.

(7) Compliance with the "No Double Standard" policy on dissemination of terrorist threat information is maintained. (See Chapter IV.)

b. Assistant Secretary of Defense for Homeland Defense (~~ASD/HD~~ ASD(HD)). The ~~F~~fiscal year 2003 National Defense Authorization Act directed the establishment of an assistant secretary of defense for homeland defense. Section 902 of Public Law 107-314, Reorganization of Office of Secretary of Defense for Administration of Duties Relating to Homeland Defense and Combating Terrorism, establishes one of the ~~A~~assistant ~~S~~secretaries as the ~~ASD/HD~~ ASD(HD) and further stipulates that he shall

have as his principal duty the overall supervision of the homeland defense activities of the Department of Defense.

~~(1) The Office of the Assistant Secretary of Defense for Homeland Defense is established within the office of the Under Secretary for Policy.~~

~~(2) In the role of providing overall supervision of homeland defense activities and civil support within Department of Defense, the ASD(HD) responsibilities include:~~

~~(a) Develop strategic planning guidance for DOD's role in Homeland Security (HLS).~~

~~(b) Develop and update force employment policy, guidance, and oversight.~~

~~(c) Serve as the DOD Domestic Incident Manager for DOD support to State and local civil authorities.~~

~~(d) Provide DOD support, as appropriate, to assist in developing capacities and capabilities of civilian agencies requisite to conducting homeland security missions.~~

~~(e) When directed, serve as the Secretary of Defense's (SecDef's) executive agent for homeland defense (HLD) and as directed, assist the Secretary in providing guidance, through the Chairman, Joint Chiefs of Staff (CJCS), to the combatant commanders for HLD missions and military activities in support to civil authorities.~~

~~(f) Provide coordination with the Office of Homeland Security.~~

(1)The principal duty of the ASD(HD) is to provide overall supervision of HD and CS activities support within DOD. In that role, the ASD(HD) responsibilities include:

(a) Developing strategic planning guidance for DOD's role in HS.

(b) Developing and updating force employment policy, guidance, and oversight.

(c) Overseeing DOD activities that provide MACA in domestic emergencies in accordance with existing national level emergency response plans and approved memoranda of understanding.

(d) Providing DOD support, as appropriate, to assist in developing capacities and capabilities of civilian agencies requisite to conduct HS missions.

(e) Serving as the DOD domestic crisis manager focusing on coordination and integration of DOD domestic crisis activities with other departments and agencies and the combatant commanders. Exceptions include those activities requiring the use of

special operations forces.

(f) Assuming responsibility for the Defense Critical Infrastructure Program (DCIP), domestic AT and FP, HD interagency coordination, HD technology transfer, NSSEs and COOP/COG.

c. The Chairman of the Joint Chiefs of Staff shall:

(1) Serve as the principal advisor to the Secretary of Defense for all DOD AT issues.

(2) Prepare joint doctrine and assist the Assistant Secretary of Defense (Special Operations and Low Intensity Conflict) [ASD (SO/LIC)] in development and maintenance of the AT program, standards and procedures. Review doctrine, policy, standards, and procedures of the DOD Components. Review, coordinate, and oversee for the Secretary of Defense and in conjunction with the DOD components and Services, the AT training for all DOD and Armed Forces personnel (including their dependent family members).

(3) Ensure the Chairman's Program Review and the Chairman's Program Assessment include a summary of AT requirements as determined by the Joint Requirements Oversight Council and derived from Combatant Commander Integrated Priority Lists.

(4) Annually, as part of the DOD ~~program and~~ Planning, Programming, ~~and~~ Budgeting, and Execution System (PPBE~~S~~) cycle, assist the Military Departments in determining the merit of AT requirement submissions. Review the adequacy of resources proposed by the Military Departments to determine whether they meet AT objectives and support Combatant Commanders' AT programs. Coordinate and make recommendations on unresolved AT requirements during programming and budget reviews. These reviews shall be done in conjunction with OSD Port Support Activities (PSAs) having resource, program, and budget oversight responsibilities for the functional areas that comprise the AT budget aggregate. Advise the Secretary of Defense of any changes needed to meet AT requirements.

(5) Assess the DOD Components' AT policies and programs for the protection of DOD elements and personnel, including DOD-owned, leased, or managed infrastructure and assets critical to mission accomplishment and other DOD-owned, leased or managed mission essential assets. Ensure assessments are conducted of Chairman of the Joint Chiefs of Staff exercises, air/sea ports of embarkation/debarkation, and in-transit forces.

(6) Assess AT as an element of the overall force planning function of any force deployment decision. Periodically reassess AT posture of deployed forces. Review Combatant Commanders' joint operation plans (OPLANS, CONPLANS, and functional plans), deployment orders, and other relevant documents for AT issues ~~considerations~~.

(7) Assess the implementation of Force Protection Conditions (FPCONs) for uniform implementation and dissemination as specified by DOD Directive 2000.12, *D~~o~~OD Antiterrorism (AT) Program*, DOD Instruction 2000.16, *D~~o~~OD Antiterrorism Standards*, and DOD Handbook O-2000.12-H, *D~~o~~OD Antiterrorism Handbook*.

(8) Provide representatives to the DOD Antiterrorism Coordinating Committee (ATCC) and appropriate subcommittees as required under enclosure 3 of D~~o~~ODD 2000.12. Provide an observer to the Overseas Security Policy Board. Appoint the Director for Operations, Joint Staff (J3) to co-chair the Antiterrorism Coordinating Committee - Senior Steering Group (ATCC-SSG) and the Deputy Director for Global Operations (Antiterrorism/Force Protection) Joint Staff to co-chair the ATCC under enclosure 3 of D~~o~~ODD 2000.12.

(9) Coordinate with the Under Secretary of Defense for Intelligence and the Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict (ASD[SO/LIC]) on sharing of terrorism intelligence and counterintelligence data and law enforcement (LE), suspicious activity report (SAR) information on AT. This includes threats posed to the DOD Components and the DOD elements and personnel by domestic and foreign terrorists.

(10) Assess the capability of the Military Departments, the Combatant Commands, and the Defense intelligence and security organizations to collect, receive, evaluate, analyze, and disseminate all relevant data on terrorist activities, trends, and indicators of imminent attack. Also assess the capability to fuse suspicious activity reports from military security, law enforcement, and counterintelligence organizations with national-level intelligence, surveillance, and reconnaissance collection activities.

(11) In coordination with the ASD(SO/LIC), manage and administer the Chairman of the Joint Chiefs of Staff CbT-RIF pursuant to Chairman of the Joint Chiefs of Staff Instruction 5261.01~~B~~C, *Combating Terrorism Readiness Initiative Fund*, July 1, 2001. Ensure ~~16~~ out-year maintenance costs for CbT-RIF-funded projects are identified and coordinated with the Military Departments so that they are addressed during the ~~PPBS~~ PPBE cycle.

(12) Maintain a centralized database of all vulnerability assessments (VAs) conducted. Prepare and disseminate analysis of DOD-wide AT vulnerability trends correlated to Military Department efforts within the ~~PPBS~~ process.

(13) Be responsible for policy guidance and oversight of the Antiterrorism Enterprise Portal (ATEP). ~~CJCS guidance is transmitted to the Director, Joint Staff, for implementation.~~

(a) ~~Antiterrorism Enterprise Portal.~~ ATEP encompasses the policies, procedures, ~~trained personnel,~~ and information systems that support trained personnel in managing the elements of an AT program, from the Joint Staff through the operating

forces and components, ~~along the entire spectrum of warfare.~~ across the range of military operations. ~~These elements include threat assessments, vulnerability assessments, planning, exercises, program reviews and training.~~ These elements include risk management, planning, training and exercises, resource generation, and comprehensive program review.

(b) The ~~Antiterrorism Enterprise Portal~~ ATEP System~~.~~ ~~A~~ is a comprehensive web enabled system that provides the Joint Staff, combatant commands, Services, Defense agencies, DOD Field Activities, subordinate ~~joint~~ task forces and components, and others with information processing and dissemination capabilities necessary for AT programs. An evolutionary acquisition and implementation strategy provides warfighters with required operational capabilities. This strategy supports operator/user participation, incremental fielding of proven technology, and shorter time periods between modernization cycles.

d. Geographic ~~C~~combatant ~~C~~commanders shall:

(1) Establish AT policies and programs for the protection of all DOD elements and personnel in their AOR, including those for whom the ~~C~~combatant ~~C~~commander assumes AT responsibility based on a memorandum of agreement (MOA) with a Chief of Mission (COM). Coordinate with the COMs in the AOR to identify all non-combatant commander DOD components and DOD elements and personnel. In instances where AT protection may be more effectively provided through the combatant commander, establish country-specific MOAs.

(2) Ensure AT policies and programs include specific prescriptive standards derived from DODI ~~Instruction~~ 2000.16, ~~*DoD Antiterrorism Standards*~~, to address specific terrorist ~~threat~~ capabilities and geographic settings, particularly regarding infrastructure critical to mission accomplishment and other DOD-owned, leased, or managed mission essential assets.

(3) ~~Exercise tactical control (TACON) (for force protection) over all DOD elements and personnel (including force protection responsibility for DOD dependent family members) (except those under the security responsibility of a COM) within the Combatant Commander's AOR. TACON (for force protection) applies to all DOD personnel assigned permanently or temporarily, transiting through, or performing exercises or training in the Combatant Commander's AOR. TACON (for force protection) is in addition to a Combatant Commander's normal exercise of operational control (OPCON) over assigned forces.~~ Establish force protection policies for all DOD personnel in the combatant commander's AOR. The geographic combatant commander's force protection policies or programs of any DOD component deployed in that command's AOR and not otherwise under the security responsibility of the DOS. Transient forces do not come under the chain of command of the area commander solely by their movement across operational area boundaries, except when the combatant commander is exercising TACON authority for force protection purposes.

(4) Periodically, assess and review the AT programs of all ~~combatant commander-a~~assigned DOD ~~C~~components in their AOR. Assess the AT programs of all DOD components performing in their AOR that are not under the ~~security~~ responsibility of a COM. ~~Military Service c~~Component commands ~~or other subordinate commands reporting to the Combatant Commander~~ may be delegated responsibility to conduct these assessments. Ensure AT program reviews include a validation of the ~~17 thoroughness of the AT~~ risk management methodology used to assess asset criticality, terrorist threat, and vulnerabilities. AT program reviews shall also evaluate installation and activity preparedness to respond to terrorist incidents (including chemical, biological, radiological, nuclear, and high-yield explosives [CBRNE] incidents), and the plans for managing the consequences of terrorist incidents and maintaining continuity of essential military operations. Relocate forces as necessary and report to the Secretary of Defense through the Chairman of the Joint Chiefs of Staff pertinent actions taken for ~~AT~~ protection.

(5) Consistent with DOD Instruction 5210.84, *Security of D~~o~~OD Personnel at US Missions Abroad*, and all appropriate memorandums of understanding (MOUs), serve as the DOD point of contact with host-nation (HN) officials on matters involving AT policies and programs ~~measures~~.

(6) Provide updates to DOD Directive 4500.54, *Official Temporary Duty Travel Abroad*, and DOD 4500.54-G, *D~~o~~OD Foreign Clearance Guide (FCG)*, stating command travel requirements and theater entry requirements.

(7) Ensure all assigned military, DOD civilians, Defense contractors, and their family members receive applicable AT training and briefings pursuant to DOD Instruction 2000.16, *D~~o~~OD Antiterrorism Standards*. Ensure personnel traveling in the AOR comply with DOD Directive 4500.54, *Official Temporary Duty Travel Abroad*, and DOD 4500.54-G, *D~~o~~OD Foreign Clearance Guide (FCG)*. Ensure personnel are aware of any Travel Warnings in effect at the time of travel. Ensure that all DOD personnel (including dependent family members) scheduled for permanent change of station to the geographic combatant commander's AOR or to another geographic combatant commander's AOR receive required AT training and briefings (e.g., AOR Updates) in compliance with DOD Instruction 2000.16. Identify and disseminate to deploying force providers specific AOR pre-deployment training requirements that all personnel must complete before arrival in theater.

(8) Identify, document, validate, prioritize, and submit to the Joint Staff the resource requirements necessary to achieve the AT program objectives for each activity under the Combatant Commander or for which that Commander has ~~AT~~ responsibility. Work with the Joint Staff and the Service component commands to ensure that resource requirements to implement the AT programs are identified and programmed according to PPB~~S~~E procedures.

(9) Establish command relationships and policies for subordinate commands, including Joint Task Forces, to ensure that effective mechanisms are in place to maintain

an AT protective posture commensurate with the terrorist threat.

(10) Assess the terrorist threat for the AOR according to this DODD Directive 2000.12 and provide threat assessment information to the DOD components and the COMs in the AOR. Develop risk mitigation measures and maintain a database of those measures and the issues that necessitated their implementation. On the basis of the threat 18 assessment, identify and designate incumbents of high-risk billets and dependent family members to receive AT resident training.

(11) Keep subordinate commanders informed of the nature and degree of the threat. Ensure that commanders are prepared to respond to changes in threats and local security circumstances. Ensure that the COMs are fully and currently informed of any threat information relating to the security of those DOD elements and personnel under their security responsibility, but not under the command of the combatant commander.

(12) Ensure compliance with the "No-Double-Standard" policy (see Chapter IV).

(13) Submit to the Chairman of the Joint Chiefs of Staff emergent and/or emergency AT requirements that cannot be funded by the Military Departments for CbT-RIF funding consideration.

(14) Ensure FPCONs are uniformly implemented and disseminated as specified by DODD 2000.12, *DoOD Antiterrorism (AT) Program*, DOD Instruction 2000.16, *DoOD Antiterrorism Standards*,, and DODD O-2000.12-H, *DoOD Antiterrorism Handbook*..

(15) Coordinate AT program issues with the functional Combatant Commanders, the COMs, the Defense Agencies, /DOD Field Activities, and the Military Departments, as appropriate.

(16) Provide a representative to the DOD ATCC and appropriate subcommittees, as required under enclosure 3 of DoODD 2000.12.

(17) Ensure a capability exists to collect, receive, evaluate, analyze, and disseminate all relevant data on terrorist activities, trends, and indicators of imminent attack. Develop and implement the capability to fuse suspicious activity reports from military security, law enforcement, and counterintelligence organizations with national-level intelligence, surveillance, and reconnaissance collection activities.

(18) Develop a geographic AOR, Combatant Commander-oriented AT Strategic Plan that details the vision, mission, goals, and performance measures in support of the Department of Defense's AT Strategic Plan.

e. Functional Combatant Commanders shall:

(1) Establish AT policies and programs for assigned DOD elements and

personnel including assessment and protection of facilities and appropriate level of AT training and briefings. Coordinate programs with the appropriate ~~Combatant Commanders~~ geographic combatant commander and ~~the~~ COM~~s~~.

(2) Coordinate with the geographic Combatant Commanders to ensure adequate AT protection of forces.

(3) Ensure that subordinate elements, which are tenant units on Military Service installations, coordinate their AT programs and requirements with the host installation commander. Differences shall be resolved through the applicable Combatant Commander and the Service component command chain of command.

(4) Identify and designate incumbents of high-risk billets and dependent family members requiring AT resident training. Provide AT resident training to personnel assigned to high-risk billets and others, as applicable.

(5) For emergent and/or emergency AT requirements that cannot be funded through other means, submit requirements to the Chairman of the Joint Chiefs of Staff for CbT-RIF consideration.

(6) Provide a representative to the DOD ATCC and appropriate subcommittees, as required under enclosure 3 of DO~~o~~DD 2000.12.

(7) Identify, document, and submit to the Joint Staff the resource requirements necessary to achieve AT program objectives for each activity under the Combatant Command or for which the ~~C~~commander has ~~AT~~ responsibility. Work with the Service component commands to ensure that resource requirements to implement the AT programs are identified and programmed according to PPB~~S~~ES procedures.

(8) Develop their own ~~a functional~~ Combatant Commander-oriented AT Strategic Plan that details the vision, mission, goals, and performance measures in support of the Department of Defense and geographic Combatant Commanders' AT Strategic Plans.

f. Directors of other Defense Agencies and DOD Field Activities, Office of the Secretary of Defense (OSD), Principal Staff Assistants, and those that report directly to the Secretary or Deputy Secretary of Defense, shall:

(1) Support the geographic Combatant Commanders as they exercise overall FP responsibility and execute their AT programs for the personnel and resources ~~for AT~~ within their respective AOR. Institute AT Programs, ensure that Defense Agencies and DOD Field Activities conduct vulnerability assessments that address terrorism as a potential threat to the DOD elements and personnel, and incorporate AT measures into contingency response plans.

(2) Utilize DOD O-2000.12-H, *D~~o~~OD Antiterrorism Handbook*, and DODI

2000.16, *DoOD Antiterrorism Standards*, for the AT planning and execution for their headquarters (HQ) and all activities under their cognizance: consider mission, characteristics of the activity, geographic location, threat level, and FPCON. Establish prescriptive AT standards for installations and facilities not located on US military installations. Coordinate with the applicable Combatant Commander to ensure AT plans and polices and programs are in concert with the geographic Combatant Commanders' overall responsibility for the AOR.

(3) Comply with DODI 2000.16, *DoOD Antiterrorism Standards*, requirements to maintain an AT training and exercise program. Ensure that all assigned personnel comply with DOD Directive 4500.54, *Official Temporary Duty Travel Abroad,* and DOD 4500.54-G, *DoOD Foreign Clearance Guide (FCG)*. Ensure that personnel are aware of any travel security advisories in effect at the time of travel. Ensure that all DOD personnel (including dependent family members) scheduled for permanent changes of station to foreign countries receive required AT training or briefing specified in DODI 2000.16.

(4) Provide members to the DOD ATCC and appropriate subcommittees, as requiredunder enclosure 3 of DODD 2000.12, *DoOD Antiterrorism (AT) Program*.

(5) As part of the PPBSE cycle, identify and document resource requirements necessary to implement and maintain AT programs. Submit AT requirements to the Secretary of Defense with an information copy to the Chairman of the Joint Chiefs of Staff and the appropriate Combatant Commanders. Include resource requirements in program and budget submissions. For emergent and/or emergency AT requirements that cannot be funded through other means, submit requirements through the appropriate Combatant Commander to the Chairman of the Joint Chiefs of Staff for CbT-RIF consideration. Implement accounting procedures to enable precise reporting of data submitted to Congress in the Congressional Budget Justification Book, including the number and cost of personnel directly supporting the Department of Defense'sDOD's AT program activities.

(6) Identify and designate incumbents of high-risk billets that are potentially high-risk targets of terrorist attacks and dependent family members requiring AT resident training. Ensure that AT resident training is provided to personnel assigned to high-risk billets and others, as applicable.

(7) Ensure that current physical security technology and security requirements are incorporated into all new contracts, where appropriate.

(8) Ensure AT protective features for facilities and installations are included in the planning, design, and execution of military and minor construction projects to mitigate AT vulnerabilities and terrorist threats (Unified Facilities Criteria [UFC] 4-010-01, *DoOD Minimum Antiterrorism Standards for Buildings*, Unified Facilities Criteria [UFC] 4-010-10 4-010-02, *DoOD Minimum Antiterrorism Standoff Distances for Buildings*, and Unified Facilities Criteria [UFC] 4-021-01, *Design and O&M: Mass*

Notification Systems).

(9) Develop an AT Strategic Plan that details the vision, mission, goals, and performance measures in support of the Department of Defense's AT Strategic Plan.

Homeland Security vs. Homeland Defense

Homeland security (HLLS) is not the same as homeland defense (HLD).

~~Homeland security~~ HS is a concerted national effort to prevent terrorist attacks within the US, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. ~~the prevention, preemption, and deterrence of, and defense against, aggression targeted at US territory, sovereignty, domestic population, and infrastructure as well as the management of the consequences of such aggression and other domestic emergencies. It is a national team effort that begins with local, state and federal organizations.~~

~~Homeland defense~~ HD is the protection of US territory, sovereignty, domestic population and defense critical infrastructure dependencies and interdependencies, against threats and aggression. ~~military attacks emanating from outside the United States.~~

g. With respect to combating terrorism and other homeland security concerns, the Department of Defense is not the lead agency, but has significant supporting roles in several areas. While in homeland ~~*defense*~~ defense ~~activities~~, missions (air, land and maritime defense) the ~~Department of Defense~~ DOD will take the lead and be supported by other Federal agencies. Section 876 of Public Law 107-296, the Homeland Security Act of 2002 states: "Nothing in this Act shall confer upon the Secretary [of Homeland Security] any authority to engage in warfighting, the military defense of the United States, or other military activities, nor shall anything in this Act limit the existing authority of the Department of Defense or the Armed Forces to engage in warfighting, the military defense of the United States, or other military activities."

~~h. There are three distinct circumstances in which Department of Defense would be involved in activities within the United States in support of the security of the nation:~~

~~(1) Extraordinary circumstances which require the Department to execute its traditional military missions. For example, combat air patrols and maritime defense operations. In these cases the Department plays the lead role and is supported by other Federal agencies. Also included in this category are cases in which the President, exercising his Constitutional authority as Commander in Chief, authorizes military action.~~

~~(2) Emergency circumstances of a catastrophic nature. For example: responding to an attack or assisting in response to forest fires, floods, hurricanes, tornados, and so forth, during which the Department may be asked to act quickly to provide capabilities that other civilian agencies do not have.~~

~~(3) Temporary circumstances, where the Department is given missions or assignments that are limited in duration or scope and other agencies have the lead from~~

~~the outset. For example, security at a special event like the Olympics, or assisting other Federal agencies in developing capabilities to detect chemical/biological threats.~~

~~i~~h. The Department of Defense established United States Northern Command (USNORTHCOM) in 2002 to consolidate under a single unified command existing missions that were previously executed by other military organizations.

(1) The command's mission is homeland defense and civil support, specifically:

~~(1)~~ (a) Conduct operations to deter, prevent, and defeat threats and aggression aimed at the United States, its territories, and interests within the assigned area of responsibility; and

~~(2)~~ (b) As directed by the President or Secretary of Defense, provide military assistance to civil authorities including consequence management operations.

~~(3)~~ (c) USNORTHCOM's ~~area of responsibility~~ AOR is America's homefront. The AOR includes air, land, and sea approaches and encompasses the continental United States (CONUS), Alaska, Canada, Mexico, Puerto Rico, the US Virgin Islands, Bermuda, St. Pierre and Miquelon Islands, and waters out to 500 nautical miles (excluding Greenland). ~~and the surrounding water out to approximately 500 nautical miles. It also includes the Gulf of Mexico, Puerto Rico, and the US Virgin Islands.~~ The defense of Hawaii and our territories and possessions in the Pacific remains the responsibility of US Pacific Command.

MILITARY ASSISTANCE TO CIVIL AUTHORITIES

A mission set of civil support following natural or manmade disasters, chemical, biological, radiological, nuclear, or high explosive consequence management, and other support as requires. Also called MACA.

With the exception of immediate responses under imminently serious conditions, any support that requires the deployment of forces or equipment assigned to a Combatant Command by Secretary of Defense Memorandum, must be coordinated with the Chairman of the Joint Chiefs of Staff. The Chairman shall evaluate each request to use Combatant Command forces or equipment to determine if there is a significant issue requiring Secretary of Defense approval. Orders providing assistance to civil authorities that are approved by the Secretary of Defense involving the use of Combatant Command forces or equipment shall be issued through the Chairman of the Joint Chiefs of Staff. Upon Secretary of Defense approval, the Secretary of the Army, when designated "the DOD Executive Agent," shall implement and oversee DOD support in accordance with such approved orders.

The Secretary of Defense is the approval authority for any requests for potentially lethal support (i.e., lethal to the public, a member of law enforcement, or a Service member) made by law enforcement agencies.

1

UNITED STATES NORTHERN COMMAND

US Northern Command plans, organizes, and executes homeland defense and civil support missions, but has few permanently assigned forces. The command will be assigned forces whenever necessary to execute missions as ordered by the President.

Approximately 500 civil service employees and uniformed personnel representing all service branches provide this essential unity of command from US Northern Command's headquarters at Peterson Air Force Base in Colorado Springs, Colo.

CHAPTER II
TERRORIST THREAT

"Terrorism is an arm the revolutionary can never relinquish."

Carlos Marighella
MINIMANUAL OF THE URBAN GUERILLA

1. ~~Overview~~ General

A critical factor in understanding terrorism is the importance of the emotional impact of the terrorist act on an audience other than the victim. This chapter provides ~~background information~~ an overview of issues dealing with ~~concerning~~ the terrorist threat ~~to enable the commander at any echelon to create and employ AT tactics, techniques, and procedures outlined in this publication~~. Terrorism has long been a media event and, as such, a phenomenon of our time. The terrorist attacks of September 11, 2001, marked a dramatic escalation in trends toward more destructive terrorist attacks and showed how vulnerable the United States is and the importance of countering terrorism ~~toward more indiscriminate targeting among international terrorists. There is an apparent shift in operational intensity from traditional sources of terrorism – state sponsors and traditional terrorist organizations – to extremist groups.~~ The new terrorist paradigm includes traditional state sponsored terrorism, well organized networks of non state actors, extremist groups and criminal networks. Moreover, they may act independently or in a well orchestrated offensive.

2. Terrorist Tactics

The general shift in tactics and methodologies among international terrorists focuses on producing mass casualties. They have raised the stakes, operating now with a more fatalistic mentality and incorporating multiple simultaneous attacks and suicide bombings. Their targets will be just as likely economic (tourists, financial networks) or agricultural ones (livestock, crops) as embassies or military forces/facilities. Their goal is not just to win favor for their causes, but can be more specifically designed to wage undeclared, unconventional war at will. The more common tactics employed by terrorist groups are discussed below.

a. Assassination. A term generally applied to the killing of prominent persons and symbolic enemies as well as traitors who defect from the group.

b. Arson. Less dramatic than most tactics, arson has the advantage of low risk to the perpetrator and requires only a low level of technical knowledge.

c. Bombing. The improvised explosive device (IED) is the terrorist's weapon of choice. IEDs can be inexpensive to produce and, because of the various detonation techniques available, may be a low risk to the perpetrator. Suicidal bombings, however, are a preferred common employment method. ~~Other a~~Advantages to these tactics include their attention-getting capacity and the ability to control casualties through time of

detonation and placement of the device. Announcing responsibility for the bombing or denying responsibility for the incident, ~~It is also easily deniable~~ should the action produce undesirable results, generates media interest and may lead to increased coverage of a terrorist groups agenda/activities.

d. Hostage Taking. This usually is an overt seizure of one or more individuals with the intent of gaining publicity, concessions in return for release of the hostages, or as human shields to increase their success in carrying out a mission. While dramatic, hostage and hostage barricade situations are risky for the perpetrator.

e. Kidnapping. While similar to hostage taking, kidnapping has significant differences. Kidnapping is usually a covert seizure of one or more specific persons in order to extract specific demands. The perpetrators of the action may not be known for a long time. News media attention is initially intense but decreases over time. Because of the time involved, successful kidnapping requires elaborate planning and logistics. The risk to the terrorist is less than in the hostage situation.

f. Hijacking or Skyjacking. Sometimes employed as a means for escape, hijacking is normally carried out to produce a spectacular hostage situation or ~~equally~~ provide a vehicle for carrying out a lethal mission. Although trains, buses, and ships have been hijacked, aircraft are the preferred target ~~because of their greater mobility and vulnerability~~.

g. Seizure. Seizure usually involves a building or object that has value in the eyes of the intended audience. There is some risk to the terrorist because security forces have time to react and may opt to use force to resolve the incident, especially if few or no innocent lives are involved.

h. Raids or Attacks on Facilities. Armed attacks on facilities are usually undertaken for one of three purposes: to gain access to radio or television broadcast capabilities in order to make a statement; to demonstrate the government's inability to secure critical facilities or national symbols; or to acquire resources (e.g., robbery of a bank or armory).

Port facilities are particularly vulnerable to terrorist sabotage.

i. Sabotage. The objective in most sabotage incidents is to demonstrate how vulnerable society is to terrorist actions. Industrialized societies are more vulnerable to sabotage than less highly developed societies. Utilities, communications, and transportation systems are so interdependent that a serious disruption of any one affects all of them and gains immediate public attention. Sabotage of industrial or commercial facilities is one means of identifying the target while making a statement of future intent. Military facilities and installations, information systems, and information infrastructures may become targets of terrorist sabotage.

j. Hoaxes. Any terrorist group that has established credibility can employ a hoax with considerable success. A threat against a person's life causes that person and those associated with that individual to devote time and effort to security measures. A bomb threat can close a commercial building, empty a theater, or delay an aircraft flight at no cost to the terrorist. False alarms dull the analytical and operational efficiency of key security personnel, thus degrading readiness.

k. Use of Special Weapons and Weapons of Mass Destruction (WMD). ~~Chemical weapons have been used by terrorists to date and there is potential for the use of both chemical and biological weapons in the future.~~ Terrorists have employed chemical and biological weapons in the past, and some terrorist organizations will seek to employ all types of CBRNE weapons when they can obtain them. These types of weapons, relatively cheap and easy to make, could be used in place of conventional explosives in many situations. The potential for mass destruction and the deep-seated fear most people have of chemical and biological weapons could be attractive to a group wishing to make the world take notice. Although an explosive nuclear device is acknowledged to be beyond the reach of most terrorist groups, a chemical or biological weapon or a radiological dispersion device using nuclear contaminants is not. The technology is simple and the cost per casualty (for biological weapons in particular) is extremely low — much lower than for ~~conventional or~~ nuclear explosives. This situation

could change as the competition for headlines increases. Increasing availability of CBRNE material, components, and weapons raises the specter of terrorists using these weapons in an attack against civilian populations or military facilities. Many chemical-biological (C-B) weapons ingredients are commercially available, and there are numerous reports throughout Europe of fissile material availability on the black market. This raises the possibility not only of terrorist use of nuclear weapons, but of radiological bombs that use fissile material to contaminate targets. Terrorists have attempted to obtain industrial radiological sources to be used in a "dirty bomb" scenario. This would result in panic, adverse economic effects, and potential health risks.

l. Environmental Destruction. Although this tactic has not been widely used, the increasing accessibility of sophisticated weapons to terrorists has the potential to threaten damage to the environment. ~~Examples would be intentional dumping of hazardous chemicals into a city's water supply, the destruction of an oil tanker, the intentional burning of an oil field, or the use of exotic insects and/or plants to poison or destroy a nation's food supplies.~~ Potential examples include intentional dumping of hazardous chemicals into the public water supply, the destruction of oil tankers causing ecological harm, destroying oil fields, or poisoning a nation's food supplies. The use of exotic insects, animals, or plants to poison or destroy the food supply or ecosystem is a potential low cost terror weapon.

~~m. Use of Technology and Weapons of Mass Effects (WME). Technology has important implications for the terrorist threat faced by DOD personnel. Infrastructure technologies provide attractive targets for terrorists who can apply a range of rudimentary and advanced attack techniques to disrupt or undermine confidence in a range of systems. WME create large scale detrimental (lethal or non-lethal, including economic) effects to military or civilian operations. Key elements of the national infrastructure, such as transportation, telecommunications, energy, banking, public health, and water supply are becoming increasingly dependent on computerized systems and linkages.~~

~~(1) These systems provide targeting opportunities for adversaries who possess even limited technological capabilities, and who have the ability to identify critical system choke points. Terrorists can apply computer generated attacks or more traditional means such as bombs or physical destruction to cause system-wide malfunctions. Interdependencies of systems, such as power and transportation, exacerbate this vulnerability. Significant disruption of power grids can have a devastating impact on air traffic control, railway operations, port operations, and emergency services such as fire and/or rescue and police. Attacks such as power outages also impact a wide segment of the population, command significant media attention and consequently provide an effective means for the terrorist to reach a "captive" audience.~~

~~(2) A range of technologies can also be employed effectively by terrorists to conduct operations. Although terrorists to date have not demonstrated significant technological innovation and have largely relied on traditional attack methods such as bombing, hostage taking, and assaults, several factors point to an increased likelihood of greater use of more sophisticated technologies. First, the wide scale proliferation of~~

military weapons and technologies that has followed the collapse of the former Soviet Union has increased the range of weapons available on international arms markets. Stand-off weapons such as shoulder-fired anti-aircraft weapons, light anti-tank weapons which have been used in attacks against US targets in the past, are attractive means of attack for a terrorist since they reduce vulnerability and increase chance of escape. Increased availability of more powerful explosives (such as the plastic explosive Semtex, which is easily concealed and difficult to detect), when combined with more sophisticated timing devices, detonators, and fuses, have provided the terrorist with much more lethal bombing capabilities.

(3) Increasing availability of CBRNE material, components, and weapons raises the specter of terrorists using these weapons in an attack against civilian populations or military facilities. Many chemical-biological (C-B) weapons ingredients are commercially available, and there are numerous reports throughout Europe of fissile material availability on the black market. This raises the possibility not only of terrorist use of nuclear weapons, but of radiological bombs that use fissile material to contaminate targets.

(4) A range of commercially available technologies can dramatically enhance terrorist operational capability. These include communications equipment, encryption capabilities, surveillance equipment, weapons, a range of computer and information management technologies, weapons components, and the Internet. The ability to acquire or adapt technologies can give terrorists an edge in choosing targets and conducting attacks as well as significantly expanding their range of attack options.

(5) Technological advances also enhance antiterrorism capabilities. Recent research and development efforts have focused on the following areas:

(a) Detection of explosives and other weapons;

(b) Detection of, and defense against, C-B agents;

(c) Physical protection (e.g., alarms, barriers, access control);

(d) Incident response; and

(e) Data analysis and dissemination.

(6) Explosive detection technologies can be applied for both airline security and for fixed facilities. They detect physical, chemical, or mechanical properties of bombs using a variety of technologies, from x-rays and radio waves to dogs and "sniffer" technologies.

(7) Detection of C-B agents poses a significant challenge, since almost anyone that can brew beer can manufacture a biological agent, and toxic chemicals are widely available on the commercial market. Laser technologies have shown promise in

~~detection of C-B agents, and research and development work on personnel protective equipment and vaccines is being pursued aggressively.~~

~~(8) A range of technologies is currently being investigated to enhance physical protection capabilities. Access control technologies, which include a range of personnel identification systems, metal detectors, and closed circuit surveillance devices are being researched and fielded on a regular basis. Barrier technologies are also being fielded, and enhancements in building design to enhance bomb resistance are being incorporated into new and existing DOD buildings in high threat areas.~~

~~(9) Incident response technologies are developed to assist in responding to assaults on facilities, hostage taking, or criminal activities. Incident response activities include disrupting the attack, defending targets, aiding persons injured in an attack, rescuing hostages, and apprehending attackers. A broad range of technologies are included in this category such as fiber-optic and low-light camera technologies, highly accurate sensors, nonlethal weapons, incapacitating agents, and software tools for profiling terrorists and supporting response planning.~~

~~(10) Effective data dissemination is a key measure to improving antiterrorism awareness and preparedness. The rapid evolution of information technology has facilitated the transfer of accurate terrorist profiles (to include photographs) and the ability to transfer the information anywhere in the world quickly. Other key AT data, such as protection technologies and procedures, can also be transmitted to field locations quickly and effectively. Recent efforts have reduced barriers between agencies on the fusion and dissemination of AT data.~~

3. Terrorist Groups

a. A terrorist group's selection of targets and tactics is also a function of the group's affiliation, level of training, organization, and sophistication. For years, security forces categorized terrorist groups according to their operational traditions — national, transnational, and international. National groups operated within the boundaries of a single nation. Transnational groups operated across international borders. International groups operated in two or more nations and were usually assumed to receive direction and support from a foreign government. Historically, ~~T~~terrorist groups have also been ~~are~~ categorized by government affiliation to help security planners anticipate terrorist targets and their sophistication of intelligence and weaponry. Three general terrorism categories are shown in Figure II-1.

Figure II-1. Categories of Terrorist Groups

b. While the three categories broadly indicate the degrees of sophistication that may be expected, it is important to examine each terrorist group on its own terms. The vast funds available to some narco-terrorists afford them the armaments and technology rivaling some nation-states. ~~Messianic r~~Religious cults or organizations have features from all three of the listed categories. They may be "non-state-supported" (e.g., Japan's Aum Shinrikyo cult or ~~the Abdul-Ramman group that perpetrated the World Trade Center bombing)~~ Al-Qaeda, "state-supported" (e.g., extremist factions of HAMAS who believe violence serves their concept of religious servitude), or "state-directed" (e.g., Hizballah is both the "Party of God" and a religious ~~cult~~ organization that employs violence in support of both religion and politics).

4. Terrorist Organization

a. Despite their diversity in motive, sophistication, and strength, terrorist organizations share a basic structure as depicted in figure II-2.

b. At the base, underlying conditions such as poverty, corruption, religious conflict and ethnic strife create opportunities for terrorists to exploit. Some of these conditions are real and some manufactured. Terrorists use these conditions to justify their actions and expand their base of support. The belief that terror is a legitimate means to address such conditions and effect political change is a fundamental problem enabling terrorism to develop and grow.

c. The international environment defines the boundaries within which terrorists' strategies take shape. ~~As a result of f~~Freer, more open borders, as well as sympathetic

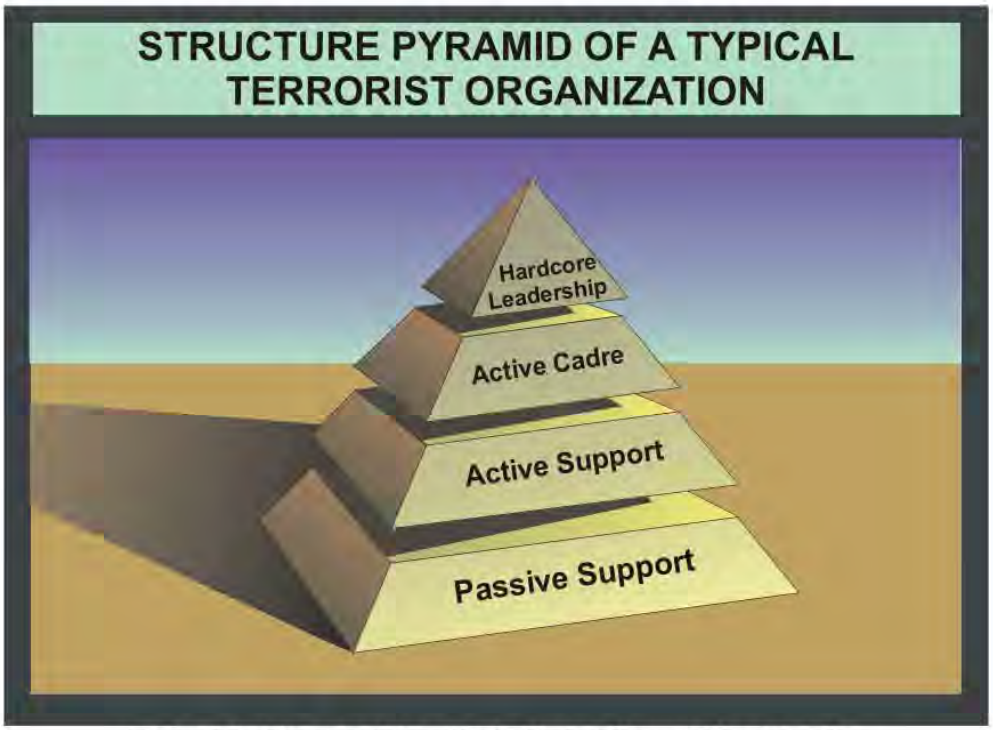

Figure II-2. Structure Pyramid of a Typical Terrorist Organization

governments ~~this environment unwittingly~~ provides terrorists access to havens, capabilities, and other support ~~to terrorists~~. ~~But access alone is not enough. Terrorists must have a physical base from which to operate.~~ Whether through ignorance, inability, or intent, states around the world still offer havens—both physical (e.g., safe houses, training grounds) and virtual (e.g., reliable communication and financial networks)—that terrorists need to plan, organize, train, and conduct their operations. Once entrenched in a safe operating environment, the organization can begin to solidify and expand. The terrorist organization's structure, membership, resources, supporters, and security determine its capabilities and reach.

d. At the top of the structure, the terrorist leadership provides the overall direction and strategy that links all these factors and thereby breathes life into a terror campaign. The leadership becomes the catalyst for terrorist action. The loss of the leadership can cause many organizations to collapse. Some groups, however, are more resilient and can promote new leadership should the original fall or fail. Still others have adopted a more decentralized organization with largely autonomous cells, making our challenge even greater.

e. While retaining this basic structure, the terrorist challenge has changed considerably over the past decade and likely will continue to evolve. Ironically, the particular nature of the terrorist threat faced today springs in large part from some of our past successes.

f. In the 1970s and 1980s, the United States and its allies combated generally secular and nationalist terrorist groups, many of which depended upon active state sponsors. While problems of state sponsorship of terrorism continue, years of sustained counterterrorism efforts, including diplomatic and economic isolation, have convinced some governments to curtail or even abandon support for terrorism as a tool of statecraft. The collapse of the Soviet Union—which provided critical backing to terrorist groups and certain state sponsors — accelerated the decline in state sponsorship. Many terrorist organizations were effectively destroyed or neutralized, including the Red Army Faction, Direct Action, and Communist Combatant Cells in Europe, and the Japanese Red Army in Asia. Such past successes provide valuable lessons for the future.

g. The end of the Cold War also saw dramatic improvements in the ease of transnational communication, commerce, and travel. Unfortunately, the terrorists adapted to this new international environment and turned the advances of the 20th century into the destructive enablers of the 21st century.

h. ~~Al-Qaida~~Al-Qaeda exemplifies how terrorist networks have twisted the benefits and conveniences of our increasingly open, integrated, and modernized world to serve their destructive agenda. The ~~al-Qaida~~Al-Qaeda network is a multinational enterprise with operations in more than 60 countries. Its camps in Afghanistan provided sanctuary and its bank accounts served as trust fund for terrorism. Its global activities are coordinated through the use of personal couriers and communication technologies emblematic of our era —cellular and satellite phones, encrypted e-mail, Internet chat rooms, videotape, and CD-~~roms~~ROMs. Like a skilled publicist, Usama bin Laden and ~~al-Qaida~~Al-Qaeda have exploited the international media to project his image and message worldwide.

i. Members of ~~al-Qaida~~Al-Qaeda have traveled from continent to continent with the ease of a vacationer or business traveler. Despite our coalition's successes in Afghanistan and around the world, some ~~al-Qaida~~Al-Qaeda operatives ~~have escaped~~ remain at large to plan additional terrorist attacks. In an age marked by unprecedented mobility and migration, they readily blend into communities wherever they move.

j. They pay their way with funds raised through front businesses, drug trafficking, credit card fraud, extortion, and money from covert supporters. They use ostensibly charitable organizations and non-governmental organizations for funding and recruitment. Money for their operations transferred surreptitiously through numerous banks, money exchanges, and alternate remittance systems (often known as "hawalas") —some legitimate and unwitting, others not.

k. These terrorists are also transnational in another, more fundamental way — their victims. Besides US citizens, ~~T~~the September 11 attacks murdered citizens from Australia, Brazil, China, Egypt, El Salvador, France, Germany, India, Israel, Jordan, Japan, Pakistan, Russia, South Africa, Switzerland, Turkey, the United Kingdom and scores of other countries.

l. As the ~~al-Qaida~~Al-Qaeda network demonstrates, the terrorist threat today is mutating into something quite different from its predecessors. Terrorists can now ~~use the~~ take full advantage of technology to disperse leadership, training, and logistics not just regionally but globally. Establishing and moving cells in virtually any country is relatively easy in a world where more than 140 million people live outside of their country of origin and millions of people cross international borders ~~every day~~ daily.

m. Furthermore, terrorist groups have become increasingly self-sufficient by exploiting the global environment to support their operations. Whether it is the Revolutionary Armed Forces of Colombia's involvement in the cocaine trade in Colombia, ~~al-Qaida~~Al-Qaeda's profiting from the poppy fields in Afghanistan, or Abu Sayyaf's kidnapping for profit in the Philippines, terrorists are increasingly using criminal activities to support and fund their terror. In addition to finding sanctuary within the boundaries of a state sponsor, terrorists often seek out states where they can operate with impunity because the central government is unable to stop them. Such areas are found in the Americas, Europe, the Middle East, Africa, and Asia. More audaciously, foreign terrorists also establish cells in the very open, liberal, and tolerant societies that they plan to attack.

~~Al-Qaida~~Al-Qaeda a.k.a. Qa'idat al-Jihad

Established by Usama Bin Ladin in the late 1980s to bring together Arabs who fought in Afghanistan against the Soviet Union. Helped finance, recruit, transport, and train Sunni Islamic extremists for the Afghan resistance. Current goal is to establish a pan-Islamic Caliphate throughout the world by working with allied Islamic extremist groups to overthrow regimes it deems "non-Islamic" and expelling Westerners and non-Muslims from Muslim countries, particularly Saudi Arabia. Issued statement under banner of "the World Islamic Front for Jihad Against the Jews and Crusaders" in February 1998, saying it was the duty of all Muslims to kill US citizens, civilian or military, and their allies everywhere. Merged with Egyptian Islamic Jihad (Al-Jihad) in June 2001.

~~Al-Qaida~~Al-Qaeda probably has several thousand members and associates. Also serves as a focal point or umbrella organization for a worldwide network that includes many Sunni Islamic extremist groups, some members of al-Gama'a al-Islamiyya, the Islamic Movement of Uzbekistan, and the Harakat ul-Mujahidin.

~~Al-Qaida~~Al-Qaeda has cells worldwide and is reinforced by its ties to Sunni extremist networks. Was based in Afghanistan until Coalition forces removed the Taliban from power in late 2001. ~~Al-Qaida~~Al-Qaeda has dispersed in small groups across South Asia, Southeast Asia, and the Middle East and probably will attempt to carry out future attacks against US interests.

~~Al-Qaida~~Al-Qaeda maintains moneymaking front businesses, solicits donations from like-minded supporters, and illicitly siphons funds from donations to Muslim charitable organizations. US efforts to block ~~al-Qaida~~Al-Qaeda funding has hampered the group's ability to obtain money.

SOURCE: United States Department of State Patterns of Global Terrorism 2002 April 2003

5. Terrorist Targets

a. It is sometimes difficult for Americans to understand why terrorism seems to thrive in the environment that offers the least justification for political violence (e.g., democracies and ineffective authoritarian regimes). Equally puzzling is the relative absence of terrorism in those societies with totalitarian and effective authoritarian governments. The reasons for this apparent paradox can be summarized as being a matter of social control. The terrorist operates covertly. In societies where little is done without the knowledge of internal security agencies, covert activity for any appreciable period of time is difficult. The same principle applies to acquisition of weapons, communications equipment, and explosives. Another factor is public information. Because the terrorist's objectives usually include gaining the attention of a target audience through a violent act, the terrorist can easily be denied that objective in an environment where information media are tightly controlled. Finally, in controlled societies, the ability of terrorist organizations to create functional networks or to move funds within the financial system is severely hindered.

b. The reasons US interests are a target for so many terrorist groups around the world are complex and must be understood in order to effectively combat terrorism in the long term. One reason some terrorist groups target the United States and its citizens is ideological differences. The United States is a leading industrial power and the leading capitalist state. These reasons are enough to incite the animosity of some groups that are committed to different social systems.

c. Of greater importance is the perception that the US Government can dictate courses of action to other governments. Terrorists think that by pressuring the United States through acts of terror, the US Government will bring pressure to bear on the targeted government to comply with terrorists' demands. Although US influence is substantial in the world community, this is not a policy of the US Government.

d. Mere presence is another factor. Americans are all over the world in capacities ranging from diplomatic service to tourists. This availability makes targeting Americans easy even for relatively poorly trained non-state-supported groups. It also

TERRORISTS AND TOURISM

The most effective fear that the terrorist can generate for the tourist is that he will never arrive at his destination — or will never return home alive. Convinced of this, a supply of tourist visitors could suddenly dry up. Expensive tourist infrastructures, depending on a constant flow of customers — margins in the tourist industry are often surprisingly slender — then lie idle. The industry is very labor intensive so a considerable unemployment problem is created . . . A pistol pointed at a hostage in an aircraft, then, could be a pistol pointed at a country's economic heart.

SOURCE: G. Norton, quoted in Chris Ryan, Tourism, Terrorism and Violence Research Institute for the Study of Conflict and Terrorism, September 1991

adds to the chances of Americans being killed or injured unintentionally. These same considerations apply to members of the US military forces with the added factor of "symbolic value." The Armed Forces are clearly visible symbols of US projection of power and presence; thus, terrorists find military personnel and installations appealing targets.

e. Terrorism is a major factor across the range of military operations. It attracts a great deal of attention and few question its actual and potential capacity to kill and destroy. The threat of terrorism in all operations is only one of many FP issues the commander must consider. The same types of acts that gain attention in peacetime military operations can hinder military operations in war (e.g., espionage, sabotage, vandalism, or theft).

f. In peacetime military operations, there is no definitive method of differentiating terrorist acts from other violent crimes because the perpetrator's intent may be the only discriminator. A rule of thumb that can be applied is if the act is obviously related to personal gain (robbery of money or high-value items) or personal motivation (hatred, love, revenge) it is a crime, but probably not terrorist-related. On the other hand, if the act appears to adversely affect military operations (communications facilities, fuel storage areas) or has a high symbolic value (headquarters, particular individuals), the crime probably has terrorist implications even when no claim is forthcoming. Recognizing the difference between acts of violence and terrorist acts is vital in order to properly understand the threat's intent and determine required defensive measures.

The American soldier is a symbol of US power and presence and is consequently an inviting target for terrorists.

65. ~~Domestic~~ Terrorism Against the Homeland

Terrorists have attacked on American soil since we became a Nation. Historically, though, the attacks were primarily committed by Americans, done infrequently, and on a generally small scale. Since the early 1990s, the scale of the attacks has increased, as has the presence of foreign terrorists (e.g., World Trade Center in 1993, Oklahoma city in 1995 [conducted by Americans], and the attacks of September 11, 2001). ~~a. On September 11, 2001, our Nation learned a terrible lesson. American soil is not immune to foreign terrorists capable of mass murder and terror. The worst of these terrorists - and target number one in our war on terrorism - is the terrorist network Al-Qaeda. Yet the threat to America is not limited to Al-Qaeda nor to suicide hijackings of commercial aircraft. The threat is much broader, as we learned on October 4, 2001, when we discovered that a life-threatening biological agent -- anthrax - was being distributed through the U.S. mail.~~

~~b~~a. ~~Unless we act to prevent it, a new wave of terrorism, potentially involving the world's most destructive weapons, looms in America's future. Today's t~~Terrorists can strike at any place, at any time, and with virtually any weapon. Securing the American homeland is a challenge of monumental scale and complexity. The 1995 bombing of the Murrah Federal Building in Oklahoma City and the attacks of 9/11 highlight~~s~~ the threat of ~~domestic~~ terrorist acts within the US ~~designed to achieve mass casualties. Both d~~Domestic terrorist groups ~~(such as the National Alliance, the Aryan Nation, and the extremist Puerto Rican separatist group Los Macheteros),~~ trans-national terrorist groups, and special interest extremist groups continue to pose a threat to the peace and stability of our country.

~~c. The terrorist threat to America takes many forms, has many places to hide, and is often invisible. Our enemies seek to remain invisible, lurking in the shadows. And while Al-Qaeda remains America's most immediate and serious threat, other international terrorist organizations, as well as domestic terrorist groups, possess the will and capability to attack the United States.~~

~~d~~b. ~~One fact dominates all domestic terrorist threat assessments: terrorists are strategic actors. They~~Terrorists choose their targets deliberately based on the weaknesses they observe in our defenses and in our preparations. They can balance the difficulty in successfully executing a particular attack against the magnitude of loss it might cause. They can monitor our media and listen to our policymakers as our Nation discusses how to protect itself - and adjust their plans accordingly. Where we insulate ourselves from one form of attack, they can shift and focus on another exposed vulnerability. We must defend ourselves against a wide range of means and methods of attack. ~~Our enemies are working to obtain chemical, biological, radiological, and nuclear weapons for the purpose of wreaking unprecedented damage on America.~~ Terrorists continue to employ conventional means of attack, while at the same time gaining expertise in less traditional

means, such as attacks on computer, banking, and utility systems. Other terrorists are working to obtain chemical, biological, radiological, and nuclear weapons for the purpose of wreaking unprecedented damage on America. Our society presents an almost infinite array of potential targets that can be attacked through a variety of methods.

~~e. The American people and way of life are primary targets of terrorists. Our population and way of life, while the source of our Nation's strength, is also a source of inherent vulnerability. Our population is large, diverse, and highly mobile, allowing terrorists to hide within our midst. Americans congregate at schools, sporting arenas, malls, concert halls, office buildings, high-rise residences, and places of worship, presenting targets with the potential for many casualties. Much of America lives in densely populated urban areas, making our major cities conspicuous targets. Americans subsist on the produce of farms in rural areas nationwide, making our heartland a potential target for agroterrorism.~~

~~f~~c. Terrorist ~~organizations~~ groups ~~have time on their side. They~~ can infiltrate organizations, groups, or geographic areas to wait, watch, and identify weaknesses and opportunities while it is much more difficult for us to do the same. This trait is made even more relevant by our reliance on habitual processes such as repetitiveness in training and in our daily lives.

~~g~~d. The US military organizes, trains, and equips forces primarily to conduct combat operations. Inherent within the combat capabilities of the Services the military rapidly responds to domestic emergencies or disasters and provides support to US civil authorities for domestic emergencies, authorized law enforcement, and other activities.

~~h. The Department of Defense cooperates with and provides support to civil authorities directed by and consistent with laws, Presidential directives, executive orders, and DOD policies and directives.~~e Military commanders are responsible to ensure that DOD resources are used as directed and consistent with laws, Presidential directives, executive orders, and DOD policies and directives,~~judiciously by adhering to the following principles:~~

~~(1) Except in the case of immediate response (see chapter 1) when local commanders can respond to save lives, prevent human suffering, or mitigate gross property damage, DOD resources are provided only when response or recovery requirements are beyond the capabilities of local, State, and Federal civil authorities and when they are requested by a lead federal agency (LFA).~~

~~(2) DOD specialized capabilities (e.g., airlift and reconnaissance) are used efficiently.~~

~~(3) The Secretary of Defense retains command of military forces providing civil support.~~

~~(4) DOD components do not perform any function of civil government unless~~

~~authorized.~~

~~(5) Unless otherwise directed by the SecDef, or where provided for by law, military operations will have priority over civil support missions.~~ (See JP 3-26, *Joint Doctrine for Homeland Security* for ~~detailed~~ guidance ~~to the Armed Forces~~ in the conduct of homeland security operations and JP 3-07.7, Doctrine for Civil Support, for guidance on military support to civil authorities.)~~in joint, multinational, and interagency environments.)~~

Intentionally Blank

CHAPTER III

INTELLIGENCE, COUNTERINTELLIGENCE, ~~AND~~ THREAT ANALYSIS AND COUNTERSURVEILLANCE

~~"... the dangers facing the United States today – ranging from chemical warfare to terrorism, regional crises, and societal turmoil – are linked in unprecedented ways and frequently span multiple countries or continents. Dealing with them therefore requires multiple intelligence disciplines, along with the combined tools of diplomacy, law enforcement, and sometimes, military force."~~"We made mistakes. Our failure to watchlist al-Hazmi and al-Mihdhar in a timely manner – or the FBI's inability to find them in the narrow window of time afforded them – showed systemic weaknesses and the lack of redundancy.

~~George J. Tenet, Director of Central Intelligence, CIA (Testimony Delivered to the Senate Select Committee on Intelligence, January 28, 1998)~~Written Statement for the Record of the Director of Central Intelligence Before the National Commission on Terrorist Attacks Upon the United States, April 14, 2004.

1. Intelligence and Counterintelligence

a. Intelligence and Counterintelligence Support. Intelligence and counterintelligence are critical in the development of ~~the first line of defense in~~ an AT program. ~~A~~ Strategic, well-planned, proactive, systematic, all-source intelligence and counterintelligence programs ~~is~~ are essential. The role of intelligence and counterintelligence is to identify the threat, provide advance warning, and disseminate critical information/intelligence in a usable form for the commander. Additionally, counterintelligence provides warning of potential terrorist attacks and provides information for CT operations. ~~This chapter provides the reader with the elements of the intelligence cycle that have particular importance in a viable AT program.~~ Effective intelligence and counterintelligence support requires effort, planning and direction, collection ~~and analysis~~, processing and exploitation, analysis and production, ~~investigations, and~~ dissemination and integration, and evaluation and feedback. The entire process is important in providing decision makers with information and timely warnings upon which to recommend ~~AT~~ FP actions.

b. Sources. The primary sources of intelligence and counterintelligence for the AT program are open-source information, criminal records, government intelligence, and local, state and federal information from continual liaison and if overseas, CI FP Source Operations, see JP 2-01.2, Joint Doctrine, Tactics, Techniques and Procedures for Counterintelligence Support to Operations, 7 May 2002. (See Figure III-1.)

Figure III-1. Sources of Intelligence and Counterintelligence

(1) Open-Source Information. This information is publicly available and can be collected, retained, and stored without special authorization. The news media are excellent open sources of information on terrorism. The news media report many major terrorist incidents and often include in-depth reports on individuals, groups, or various government counterstrategies. Government sources include congressional hearings; publications by Defense Intelligence Agency (DIA), Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), and DOS; and the national criminal justice reference services. Additionally, there are private data services that offer timely information on terrorist activities worldwide. Terrorist groups and their affiliates may also have manuals, pamphlets, and newsletters that reveal their objectives, tactics, and possible targets. Open sources are not a substitute for classified capabilities, but they can provide a valuable foundation and context for rapid orientation of the analyst and the consumer and for the establishment of collection requirements which take full advantage

of the unique access provided by classified sources.

(2) Criminal Records. Both military and civil law enforcement agencies collect criminal records. Because terrorist acts are criminal acts, criminal records are a major source for terrorist intelligence. Commanders must work through established law enforcement liaison channels because the collection, retention, and dissemination of criminal records are regulated. Local military criminal investigative offices of the US Army Criminal Investigations Command (USACIDC), Naval Criminal Investigative Service (NCIS), Air Force Office of Special Investigations (AFOSI), and Headquarters, US Marine Corps, Criminal Investigations Division, maintain current information that will assist in determining the local terrorist threat. See DOD Directive 5200.27 on proper handling of this information.

(3) Government Intelligence. The Community Counterterrorism Board. which manages the Interagency Intelligence Committee on Terrorism under the Director of Central Intelligence (DCI), is the organization that links all 60-plus federal intelligence, defense and civilian agencies involved in counterterrorism.. These agencies include the CIA (lead agency), DIA, National Security Agency, DOS, Department of Justice (DOJ), FBI, the Department of Energy (DOE), the Department of Transportation (DOT), United States Coast Guard (USCG), Federal Aviation Administration (FAA), Federal Communications Commission, Department of Homeland Security (DHS), and DOD. In response to the terrorist attacks of September 11, the terrorist Threat Integration Center was created. This new center merges and analyzes terrorist-related information collected domestically and abroad in order to form the most comprehensive possible threat picture. It includes DOD representation. Lastly, the FBI has a national Joint Terrorism Task Force (JTTF) which includes nearly 30 agencies, spanning the fields of intelligence, public safety, and federal, state, and local law enforcement. The National JTTF collects terrorism information and intelligence and funnels it to the 66 local and state JTTFs. The DOD is represented at the national level and many of the state and local JTTFs have Service representation from nearby military installations. Service intelligence and counterintelligence production organizations that compile comprehensive intelligence and counterintelligence from these agencies for distribution on a need-to-know basis throughout the Services include: the Army Counterintelligence Center; the ~~Navy Antiterrorism Alert Center~~Multiple Threat Alert Center; Headquarters, US Marine Corps, Counterintelligence; and Headquarters, AFOSI. In combatant commands, the J-2 is responsible for the integration of intelligence policy issues ~~across the command staff~~. The counterintelligence support officer (CISO) provides counterintelligence interface among the combatant command, the component commands, and the Joint Staff.

(4) Local Information. Other valuable sources of information are the individual Service member, civil servant, family member, and individuals with regional knowledge such as college faculty or members of cultural organizations. Local crime or neighborhood watch programs can also be valuable sources of information and can serve as a means to keep individuals informed in dispersed and remote areas. Intelligence exchanges with local government agencies through cooperative arrangements can also

augment regional information.

c. Responsibilities of Intelligence Agencies and Activities

(1) General. The FBI is responsible for collecting and processing

~~Al-Qaida~~Al-Qaeda a.k.a. Qa'idat al-Jihad

Established by Usama Bin Ladin in the late 1980s to bring together Arabs who fought in Afghanistan against the Soviet Union. Helped finance, recruit, transport, and train Sunni Islamic extremists for the Afghan resistance. Current goal is to establish a pan-Islamic Caliphate throughout the world by working with allied Islamic extremist groups to overthrow regimes it deems "non-Islamic" and expelling Westerners and non-Muslims from Muslim countries, particularly Saudi Arabia. Issued statement under banner of "the World Islamic Front for Jihad Against the Jews and Crusaders" in February 1998, saying it was the duty of all Muslims to kill US citizens, civilian or military, and their allies everywhere. Merged with Egyptian Islamic Jihad (Al-Jihad) in June 2001.

~~Al-Qaida~~Al-Qaeda probably has several thousand members and associates. Also serves as a focal point or umbrella organization for a worldwide network that includes many Sunni Islamic extremist groups, some members of al-Gama'a al-Islamiyya, the Islamic Movement of Uzbekistan, and the Harakat ul-Mujahidin.

~~Al-Qaida~~Al-Qaeda has cells worldwide and is reinforced by its ties to Sunni extremist networks. Was based in Afghanistan until Coalition forces removed the Taliban from power in late 2001. ~~Al-Qaida~~Al-Qaeda has dispersed in small groups across South Asia, Southeast Asia, and the Middle East and probably will attempt to carry out future attacks against US interests.

~~Al-Qaida~~Al-Qaeda maintains moneymaking front businesses, solicits donations from like-minded supporters, and illicitly siphons funds from donations to Muslim charitable organizations. US efforts to block ~~al-Qaida~~Al-Qaeda funding has hampered the group's ability to obtain money.

SOURCE: United States Department of State Patterns of Global Terrorism 2002 April 2003

domestic terrorist information to protect the United States from terrorist attack. Overseas, terrorist intelligence is principally a CIA responsibility, but the DOS, DIA, and host nation (HN) are also active players. Military intelligence activities are conducted in accordance with (IAW) Presidential Executive orders, Federal law, status-of-forces agreements (SOFAs), MOUs, and applicable Service regulations.ril 2003

(2) Intelligence Activities.

(a) The combatant commander, through the ~~commander's~~ J-2, Joint Intelligence Center, ~~and~~ the CISO, and in consultation with DIA, CIA, ~~embassy staff,~~ US country team, and applicable host-nation authorities, obtains intelligence and counterintelligence specific to the operational area and issues intelligence and counterintelligence reports, advisories, and assessments ~~to the units within the combatant command's control or operating within the combatant command's AOR~~. This network is

the backbone for communicating intelligence and counterintelligence information, advisories, and warning of terrorist threats throughout the region.

(b) DODD 2000.12, *DoDD Antiterrorism (AT) Program*, tasks the Secretaries of the Military Departments to ensure Service component commands have the capability to collect, receive, evaluate, analyze, and disseminate all relevant data on terrorist activities, trends, and indicators of imminent attack, and to develop the capability to fuse suspicious activity reports from military security, law enforcement, and counterintelligence organizations with national-level intelligence, surveillance, and reconnaissance collection activities.

(c) DODD 5105.67, *Department of Defense Counterintelligence Field Activity (DoDD CIFA)*, 2/19/2002 tasks the Secretaries of the Military Departments to:

1. Support the DOD CIFA in implementing Presidential Decision Directive/National Security Council-75, ~~U.S.~~US *Counterintelligence Effectiveness, Counterintelligence for the 21st Century*, December 28, 2000, in integrating the Defense Counterintelligence (CI) Program DOD-wide, and in overseeing the appropriate functional aspects of the program.

2. Report all significant CI activities, including investigations and operations, to the Director, DOD CIFA.

(d) DOD CIFA Antiterrorism Responsibilities:

1. Establish a threat analysis capability designed to collect, fuse and analyze domestic law enforcement information with foreign intelligence and counterintelligence information in support of the DOD CbT mission. As a designated DOD law enforcement and counterintelligence activity, CIFA shall support the efforts of the DIA Joint Intelligence Task Force for Combating Terrorism (JITF-C~~b~~T), serving as the bridge between intelligence related to international terrorism and domestic law enforcement information.

2. Maintain a domestic law enforcement database that includes information related to potential terrorist threats directed against the Department of Defense.

3. Support the ~~JITF-CbT~~JITF-CT, the combatant commands, and the military Services in preparing threat assessments and advisories.

4. Conduct specific risk assessments in support of the Defense Critical Infrastructure ~~Protection~~ Program. Identify and maintain a database of critical DOD assets and infrastructure. This database shall include vulnerability assessments of all DOD facilities.

5. Support DOD counterintelligence components in preparing threat assessments by providing tailored analytical and data-mining services.

6. Establish and manage DOD Force Protection Detachments at high-threat in-transit locations overseas, ensuring required counterintelligence and force protection support is provided to DOD Elements transiting these locations.

7. Assign DOD counterintelligence and criminal investigative personnel to the National Joint Terrorism Task Force and designated Joint Terrorism Task Forces within CONUS. Provide program oversight and coordination for assigned counterintelligence assets and serve as the repository for information obtained.

8. Provide countersurveillance support to the combatant commands upon request, subject to the approval of the Chairman of the Joint Chiefs of Staff.

9. Provide a member to the DOD ATCC and subcommittees as required~~, pursuant to enclosure 3 of this Directive.~~

10. Assist the DIA in the execution of its diplomatic security function. Such assistance shall include:

a. Representation at the National Security Council's Overseas Security Policy Board and other related committees, subcommittees, and working groups.

b. Support the DIA security assistance visits and vulnerability assessments for all DOD Elements under the security responsibility of the COMs.

(e) Each Military Department intelligence agency is responsible for the following:

1. Provide overall direction and coordination of the Service counterintelligence effort.

2. Operate a 24-hour operations center to receive and disseminate worldwide terrorist threat information to and from the combatant command J-2s, applicable Service staff elements, subordinate commands, and national agencies.

3. Provide Service commanders with information on terrorist threats concerning their personnel, facilities, and operations.

4. With the FBI or host-nation authorities, investigate terrorist incidents for intelligence, counterintelligence, and force protection aspects.

5. Provide terrorist threat information in threat briefings.

6. Conduct liaison with representatives from Federal, State, and local agencies as well as host-nation agencies to exchange information on terrorists.

7. Provide international terrorism summaries and other threat information to supported commanders. On request, provide current intelligence and counterintelligence data on terrorist groups and disseminate time-sensitive and specific threat warnings to appropriate commands.

Success in thwarting terrorist activities requires a coordinated intelligence effort from several US government agencies.

(f) Investigative Agencies. Service criminal investigative services (e.g., USACIDC, NCIS, AFOSI) collect and evaluate criminal information and disseminate terrorist-related information to supported installation and activity commanders as well as to the Service lead agency. As appropriate, criminal investigative elements also conduct liaison with local military police or security forces and civilian law enforcement agencies.

(g) Intelligence staff elements of commanders at all echelons will:

1. Promptly report all actual or suspected terrorist incidents, activities, and early warnings of terrorist attack to supported and supporting activities, the local counterintelligence office, and through the chain of command to the Service lead agency.

2. Initiate and maintain liaison with the security forces or provost marshal's office, local military criminal investigative offices, local counterintelligence offices, security offices, host-nation agencies, and (as required or

allowed by law or policy) other organizations, elements, and individuals.

3. In cooperation with the local counterintelligence offices, develop and present terrorism threat awareness briefings to all personnel within their commands.

(h) Law enforcement staff elements will be responsible for the following:

1. Report all actual or suspected terrorist incidents or activities to their immediate commander, supported activities, and Service lead agency through established reporting channels.

2. Initiate and maintain liaison with local counterintelligence offices and military criminal investigative offices.

3. Maintain liaison with Federal, host-nation, and local law enforcement agencies or other civil and military AT agencies as appropriate.

(i) Installation, base, ship, unit, and port security officers will be responsible for the following:

1. Report all actual or suspected terrorist incidents or activities to their immediate commander, supporting military law enforcement office, other supported activities, local counterintelligence office, and local military criminal investigation office.

2. Conduct regular liaison visits with the supporting military law enforcement office, counterintelligence office, and local criminal investigation office.

3. Coordinate with the supporting military law enforcement office and counterintelligence offices on their preparation and continual updating of the threat assessments.

4. Assist in providing terrorism threat awareness training and briefings to all personnel and family members as required by local situations.

d. Information Requirements. To focus the threat analysis, intelligence and counterintelligence officers develop information requirements (IRs) for identifying potential terrorist targets based on existing knowledge of an organization. Terrorist group IRs are shown in Figure III-2.

Figure III-2. Information Requirements

2. Threat ~~Assessment~~ Analysis

a. ~~Terrorist threat analysis is a continual process of compiling and examining all available information in order to identify terrorist targeting of US interests. A vulnerability analysis is a continual process of compiling and examining information on the security posture of a facility. The threat analysis is then paired with the facility's vulnerability analysis to create the threat and vulnerability assessment. Threat analysis is an essential step in identifying probability of terrorist attack. To enhance this capability to collect and analyze information from many sources, DIA maintains a terrorism data base on the Migration Defense Intelligence Threat Data System and the combatant command's J-2; the CISO, in consultation with DIA, focuses this data base information and regional information toward the intelligence and counterintelligence needs specific to the security of the command. Country threat assessments and information about terrorist organizations, biographies, and incidents in the database are disseminated to the commands and Services.~~ Terrorism threat analysis is a continual process of compiling and examining all available information concerning potential terrorist activities by terrorist groups that could target the DOD Components or the DOD Elements and Personnel. A threat analysis shall review the factors of a terrorist group's existence, capability, intentions, history, and targeting, as well as the security environment within which friendly forces operate. Threat analysis is an essential step in identifying probability of terrorist attack and results in a terrorism threat assessment. A vulnerability assessment is an evaluation to determine the vulnerability to a terrorist attack against an installation, unit, exercise, port, ship, residence, facility or other site. The threat assessment, and vulnerability assessment are then utilized with the criticality assessment to provide the commander with the basis for their risk management decisions. The commander must determine which assets require the most protection and where future expenditures are required to minimize risk of attack or lessen the severity of the outcome of an attack. To enhance this capability, which requires the collection and analysis of information from, many sources DIA maintains a terrorism database on the Migration Defense Intelligence Threat Data system. The combatant command's J-2, the CISOs, in consultation with DIA, focuses this database information and regional information toward the intelligence and counterintelligence needs specific to the security of the command. Country threat assessments and information about terrorist organizations, biographies, and incidents in the database are disseminated to the commands and services. Commands at all echelons then augment or refine the DIA's analyses to focus on their area of interest. This process is operative across the range of military operations, promotes coordination between all levels of the intelligence, counterintelligence, and law enforcement communities, ~~broadens acquisition channels,~~ and enhances timely distribution of information to the supported commander.

(1) Several factors complicate intelligence and counterintelligence collection and operations. The small size of terrorist groups, coupled with their mobility and cellular organization, make it difficult to identify the members. Unlike other criminals, terrorist cadres often receive training in counterintelligence and security measures from foreign intelligence agencies or other terrorists. Additionally, the traditional orientation of police organizations is toward individual criminals, while

military intelligence organizations focus on conventional forces. It is worth nothing that the terrorist attacks against the Office of the Program Manager-Saudi Arabian National Guard in 1995, Khobar Towers in 1996 and the USS Cole in 1998 all occurred when those areas were in THREATCON Bravo. In fact, the THREATCON was lowered from Charlie to Bravo approximately 45 days prior to the attack against Khobar Towers. Terrorist activity, therefore, requires some degree of reorientation for police and military intelligence and counterintelligence collection and operations.

(2) The ability of an intelligence system to provide critical and timely information to the user depends not only on efficient collection and processing, but also on the ability to organize, store, and rapidly retrieve this information. This capability, coupled with early warning, careful observation, and assessment of threat activity, enhances the probability of accurately predicting the types and timing of terrorist attacks.

(3) Commanders must carefully exercise judgment in estimating both the existing terrorist threat and the need for changes in antiterrorism measures. See Appendix A.

b. Having obtained a threat analysis, the commander and staff proceed to complete the threat assessment by conducting the vulnerability (Appendix B) and criticality (Appendix C) ~~and vulnerability (Appendix B)~~ assessments.

c. Drills and Exercises. Multi-echelon wargaming of possible terrorist attacks is

- There were at least four separate terrorist identity databases at State, CIA, Department of Defense, and FBI. None were interoperable or broadly accessible.
- There were dozens of watchlists, many haphazardly maintained.
- There were legal impediments to cooperation across the continuum of criminal and intelligence operations. It was not a secret, we all understood it, but little action was taken by anyone to create a common arena of criminal and intelligence data that we all could access.

But most profoundly we lacked a government wide capability to integrate foreign and domestic knowledge, data, operations, and analysis.

Warning is not good enough without the structure to put it into action.

- We all understood Bin Ladin's intent to strike the homeland but were unable to translate this knowledge into an effective defense of the country.
- Doing so would have complicated the terrorists' calculation of the difficulty in succeeding in a vast open society that was, in effect, unprotected on September 11.

During periods of heightened threat, we underlook smart, disciplined actions, but ultimately all of us must acknowledge that we did not have the data, the span of control, the redundancy, the fusion, or the laws in place to give us the chance to compensate for the mistakes that will be made in any human endeavor. This is not a clinical excuse – 3,000 people died. In the end, one thing is clear. No matter how hard we worked – or how desperately we tried – it was not enough. The victims and the families of 9/11 deserve better.

the best test, short of an actual incident, to analyze the ability of an installation, base, ship, unit, airfield, or port to respond. Drills and exercises test suspected vulnerabilities and AT measures. These exercises and drills also train the staff as well as reaction force leadership and help maintain a valid threat assessment by identifying and adjusting to changing threat capabilities as well as ~~installation, base, ship, unit, or port~~ known vulnerabilities.

3. Countersurveillance

a. Countering terrorist surveillance successfully necessitates commanders and security planners to understand the purpose of terrorist surveillance, know what terrorists look for, and know how they conduct surveillance operations. With this basic knowledge, commanders can then implement protective countermeasures, comply with DOD standardized reporting procedures, and in the end deter, detect, disrupt, and defend against future attacks.

b. Vulnerability assessment. Terrorists conduct surveillance to determine a target's suitability for attack by assessing the capabilities of existing security systems and discerning weaknesses for potential exploitation. Terrorists closely examine security procedures, such as shift changes, access control, and roving patrols; citizenship of security guards; models and types of locks; presence of closed-circuit cameras; and guard dogs. After identifying weaknesses, terrorists plan their attack options at the point or points of greatest vulnerability.

c. Terrorist surveillance techniques. The basic methods of surveillance are "mobile" and "fixed" (or static).

(1) Mobile surveillance entails active participation by the terrorists or operatives conducting surveillance, usually following as the target moves. Terrorists conduct mobile surveillance on foot, in a vehicle, or by combining the two. Mobile surveillance usually progresses in phases from a stakeout, to a pick up and then through a follow phase until the target stops. At this point operatives are positioned to cover logical routes to enable the surveillance to continue when the target moves again.

(2) Terrorists conduct fixed or static surveillance from one location to observe a target, whether a person, building, facility, or installation. Fixed surveillance often requires the use of an observation point to maintain constant, discreet observation of a specific location. Terrorists establish observation posts in houses, apartments, offices, stores, or on the street. A mobile surveillance unit, such as a parked car or van, can also serve as an observation post. Terrorists often park outside a building, facility, or installation to observe routines of security and personnel coming and going. Terrorists also use various modes of transportation to include buses, trains or boats or move by foot to approach and observe installations.

d. Protective countermeasures. The incorporation of visible security cameras, motion sensors, working dog teams, random roving security patrols (varying size, timing, and routes), irregular guard changes, and active searches (including x-ray machines and explosive

detection devices) of vehicles and persons at entry points will improve a facilities' situational awareness and present a robust force protection posture that dramatically inhibits terrorist surveillance efforts. The emplacement of barriers, roadblocks, and entry mazes that are covered by alert security forces will provide additional deterrence as these measures increase standoff and improve security force reaction time in the event of an attack. The implementation of unannounced random security measures such as 100% identification of all personnel entering the facility / installation, conducting inspections and searches of personnel and vehicles, and visible displays of vehicles mounted with crew served weapons will increase uncertainty and thus the risk of failure in the minds of terrorists.

e. Surveillance detection. Because terrorists must conduct surveillance--often over a period of weeks, months, or years--detection of their activities is possible. Regardless of the level of expertise, terrorists invariably commit mistakes. Knowing what to look for and to be able to distinguish the ordinary from the extraordinary are keys to successful surveillance detection. For these reasons, overt surveillance detection in its most basic form is simply watching for persons observing personnel, facilities, and installations.

(1) The objectives of overt surveillance detection measures are to record the activities of persons behaving in a suspicious manner and to provide this information in a format useable by the appropriate law enforcement or intelligence officials. It is important to note that overt surveillance detection emphasizes the avoidance of interpersonal confrontations with suspicious individuals unless exigent situations necessitate otherwise. Depending upon the circumstances or trends, commanders and senior law enforcement officials in coordination with intelligence experts through installation threat working groups may determine the need for more specialized covert countersurveillance measures to assure installation protection.

(2) For surveillance detection efforts to achieve positive results, military police/security forces should immediately report incidents of surveillance and suspicious activities by providing detailed descriptions of the people, the times of day, the locations, the vehicles involved, and the circumstances of the sightings to their respective criminal investigative services or counterintelligence elements for incorporation into reports such as Air Force Talon or the Naval Criminal Investigative Service Suspicious Incident Report. The incident reports are important pieces of information that over time combined with other similar sightings allow investigators to assess the level of threat against a specific facility, installation, or geographic region.

(3) The emphasis of surveillance detection is on indicators and warnings of terrorist surveillance activities. Surveillance detection efforts should focus on recording, then reporting incidents similar to the following:

(a) Multiple sightings of the same suspicious person, vehicle, or activity, separated by time, distance, or direction.

(b) Possible locations for observation post use.

(c) Individuals who stay at bus / train stops for extended periods while buses / trains come and go.

(d) Individuals who carry on long conversations on pay or cellular telephones.

(e) Individuals who order food at a restaurant and leave before the food arrives or who order without eating.

(f) Joggers who stand and stretch for an inordinate amount of time.

(g) Individuals sitting in a parked car for an extended period of time.

(h) Individuals who don't fit into the surrounding environment by wearing improper attire for the location (or season).

(i) Individuals drawing pictures / taking notes in an area not normally of interest to a standard tourist or showing interest in or photographing security cameras, guard locations, or noticeably watching security reaction drills and procedures.

(j) Individuals who exhibit unusual behavior such as staring or quickly looking away from individuals or vehicles as they enter or leave designated facilities or parking areas.

(k) Terrorists may also employ aggressive surveillance by false phone threats, approaching security checkpoints to ask for directions, or "innocently" attempting to smuggle non-lethal contraband through checkpoints. Clearly, the terrorists intend to determine firsthand the effectiveness of search procedures and to gauge the alertness and reaction of security personnel.

(4) It is important to highlight that the above surveillance indicators are recorded overtly and while performing normal military police/security forces activities. The intent is to raise the awareness of our military police/security forces to record and report the unusual during the course of routine law enforcement and security duties.

f. Reporting terrorist surveillance indicators. Implementing effective security countermeasures and employing overt surveillance detection principles will deter terrorist surveillance. However, regardless of the capabilities of a facility or installation to resource AT protective measures, good working relationships with local, state, and federal law enforcement agencies are essential to establishing cohesive, timely and effective responses to the indicators of terrorist activity. Commanders should coordinate and establish partnerships with local authorities (i.e. installation threat working groups) to develop intelligence and information sharing relationships to improve security for the installation and the military

community at large. For those occasions when the indicators of terrorist surveillance continue despite well executed overt security countermeasures the objectives should be to provide detailed reports of the indicators of surveillance to the appropriate law enforcement agency or intelligence activity. As reports of suspicious activity increase and the trends clearly indicate pre-operational terrorist surveillance, it may be necessary for commanders in coordination with senior law enforcement and intelligence officials to implement more sophisticated, uniquely-tailored countersurveillance solutions and assets to investigate the circumstances. Specialized countersurveillance assets should be coordinated and vetted by forwarding requests through the chain of command via pre-determined service or combatant command request procedures.

Intentionally Blank

CHAPTER IV
LEGAL CONSIDERATIONS

"~~US forces will act unilaterally and in concert with security partners, using all means authorized by the President and the Congress to counter international terrorism at home and abroad.~~"To defeat terrorists we will support national and partner nation efforts to deny state sponsorship, support, and sanctuary to terrorist organizations. We will work to deny terrorists safe havens in failed states and ungoverned regions. Working with other nations' military and other governmental agencies, the Armed Forces help to establish favorable security conditions and increase the capabilities of partners. The relationships developed in these interactions contribute to a global antiterrorism environment that further reduces threats to the United States, its allies, and its interests.

National Military Strategy of the United States of America, ~~1997~~ 2004

1. Authority

a. Criminal Actions. Terrorist acts committed in the US or committed outside the US against US persons or property are federal crimes whether committed during peacetime or in military operations. ~~Most terrorist acts are federal crimes whether committed during peacetime or in military operations.~~ By definition, terrorists do not meet the four requirements necessary for combatant status (wear uniforms or other distinctive insignia, carry arms openly, be under command of a person responsible for group actions, and conduct their operations in accordance with the laws of war). Only combatants can legitimately attack proper military targets. For this reason, captured terrorists are not afforded the protection from criminal prosecution attendant to prisoner of war status. ~~However, Article III of the 1949 Geneva Conventions, which requires that noncombatants be treated in a humane manner, also applies to captured terrorists.~~ However, detained terrorist will be treated humanely, as outlined in appropriate regulations, and consistent with the Geneva Conventions.

b. Jurisdiction. Most terrorist acts may be prosecuted as criminal acts violating local criminal, state, federal, or international laws. In an internationally recognized war or hostilities short of war (regional or global), terrorists can also be tried under military jurisdiction by either a court-martial, if applicable, or military commission. In peacetime military operations, most terrorist acts are federal crimes. This is also true in police actions to maintain a legitimate government. However, in an internationally recognized war or hostilities short of war (regional or global), terrorists can be tried under local criminal law or under military jurisdiction by either a court-martial or military commission.

c. Commander's Authority. A commander's responsibility and ~~authority~~ accountability to enforce security measures to protect persons and property is paramount during any level of conflict. Commanders ~~must coordinate~~ should confer with their legal advisers to determine the extent of their authority to combat terrorism.

2. Limits of Military and Intelligence Support to Civil Authorities

a. General. The fundamental restriction on the use of the military in law enforcement is contained in the Posse Comitatus Act (PCA), (18 USC 1385). However, several of the exceptions to the PCA are relevant to DOD's contribution to the fight against terrorism. The Posse Comitatus Act does not apply to the navy and Marine Corps as a matter of law. However, DOD directives and Secretary of the Navy instructions apply similar restrictions pursuant to 10 USC 375. Similarly, the USCG retains law enforcement authority in accordance with 14 USC 89 and its assignment to DHS.

(1) Constitutional Exceptions. The President, based on his inherent authority as the Executive, has the authority to use ~~the~~ military forces in cases of emergency and to protect ~~federal functions and property~~ national security. ~~In the case of civil disturbances, which may result from a terrorist act, military commanders may rely on this authority, however, the employment of active duty military forces in domestic civil disturbances may be authorized only by the President through an Executive order directing the Secretary of Defense to act in a specified civil jurisdiction under specific circumstances.~~

(2) Immediate Response. Immediate Response. Any form of immediate action taken by a DOD component or military commander to assist civil authorities or the public to save lives, prevent human suffering, or mitigate great property damage under imminently serious conditions occurring where there has not been any declaration of major disaster or emergency by the President or attack. ~~Immediate Response is that action authorized to be taken by a military commander or by responsible officials of other DOD Agencies to provide support to civil authorities to prevent human suffering, save lives, or mitigate great property damage~~. Under these circumstances, support elements must advise the DOD Executive Secretary (EXECSEC) through command channels by the most expeditious means available and seek approval or additional authorizations. The EXECSEC will notify SecDef, the Chairman of the Joint Chiefs of Staff (CJCS), and any other appropriate officials ~~Any commander or DOD official acting under "Immediate Response" authority shall advise the Joint Director of Military Support (JDOMS) through command channels by the most expeditious means available and shall seek approval or additional authorization as needed~~ (see Figure IV-1).

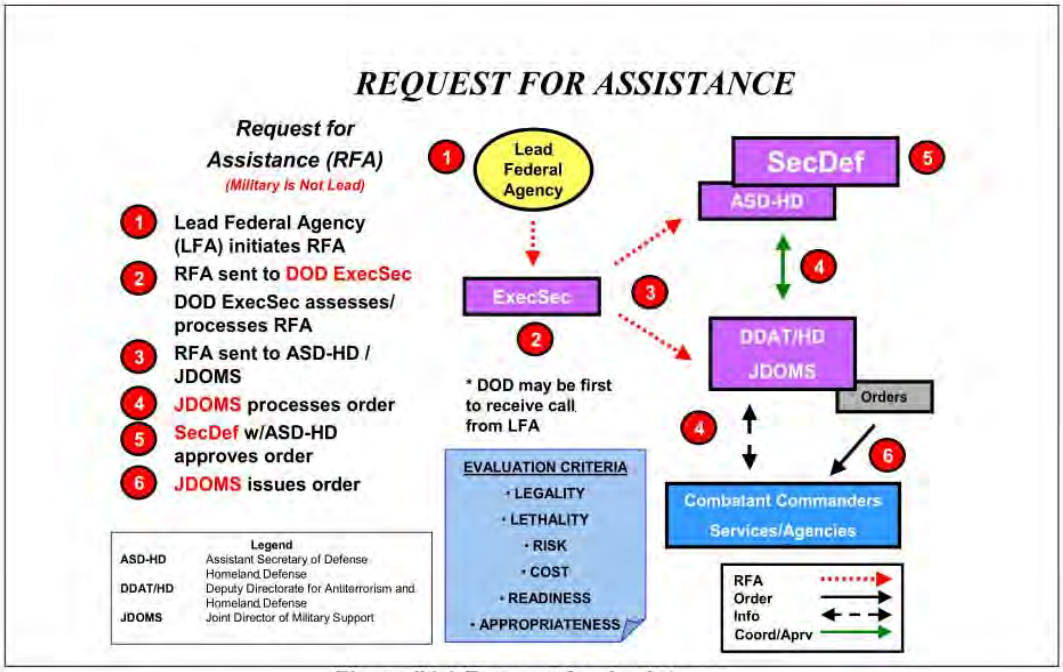

Figure IV-1 Request for Assistance

(a) In the event of imminent serious conditions resulting from any civil emergency or attack, all military commanders are authorized to respond to requests from the civil sector to save lives, prevent human suffering, or ~~limit~~ mitigate great property damage. This immediate assistance by commanders will not take precedence over their combat and combat support missions, nor over the survival of their units. Military commanders will notify the ~~DOD Executive Agent~~ JDOMS through their senior commander by the most expeditious means and seek guidance for continuing assistance whenever DOD resources are committed under Immediate Response circumstances.

(b) Immediate Response is situation-specific and may or may not be associated with a declared or undeclared disaster. These actions do not supplant established DOD plans for providing support to civil authorities. Commanders may use Immediate Response authority to assist in the rescue, evacuation, and emergency medical treatment of casualties, the maintenance or restoration of emergency medical capabilities, and the safeguarding of public health. They may provide emergency explosive ordnance disposal (EOD) service and use military working dog (MWD) teams to that end or to aid in locating lost persons. Commanders may also assist with the emergency restoration of essential public services and utilities. This may include fire fighting, water supplies, communications facilities, transportation means, electrical power, and fuel. They may also consider providing immediate assistance to assist public officials in emergency clearance of debris, rubble, and explosive ordnance from public facilities and other areas to permit rescue or movement of people and restoration of essential services. Commanders should recognize, however, that this is not a blanket provision to provide assistance. Such requests are time-sensitive and should be received from local government officials within 24 hours following completion of a damage assessment.

Commanders will always consider the impact that providing immediate response would have on their military mission requirements and not jeopardize them.

(c) When a calamity or extreme emergency renders it dangerous to wait for instructions from the proper military department, a commander may take whatever action the circumstances reasonably justify. However, the commander must comply with the following:

1 Document all facts and surrounding circumstances to meet any subsequent challenge of impropriety.

2 Retain military response under the military chain of command.

Immediate Response

Requests for an immediate response (i.e., any form of immediate action taken by a DoOD Component or military commander to save lives, prevent human suffering, or mitigate great property damage under imminently serious conditions) may be made to any Component or Command. The DoOD Components that receive verbal requests from civil authorities for support in an exigent emergency may initiate informal planning and, if required, immediately respond as authorized in DoOD Directive 3025.1. Civil authorities shall be informed that verbal requests for support in an emergency must be followed by a written request. As soon as practical, the Component or Command rendering assistance shall report the fact of the request, the nature of the response, and any other pertinent information through the chain of command to the DoOD Executive Secretary, who shall notify the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, and any other appropriate officials. If the report does not include a copy of the civil authorities' written request, that request shall be forwarded to the DoOD Executive Secretary as soon as it is available.

DODD 3025.15, Feb.18, 1997

3 Limit military involvement to the minimum demanded by necessity.

(3) Statutory Exceptions. 10 USC §§ 331-334 (Sec. 331. Federal aid for State governments; Sec. 332. Use of militia and armed forces to enforce Federal authority; Sec. 333. Interference with State and Federal law; Sec. 334. Proclamation to disperse) ~~are the primary statutory exceptions pertinent to terrorism scenarios~~. A terrorist incident may well qualify as a civil disturbance. Triggering these statutes permits the active component to take on law enforcement function, subject to policy considerations. Additional statutory exceptions to some lesser known statutes that contain exceptions to the PCA are:

(a) To assist the Department of Justice in cases of offenses against the President, Vice President, members of Congress, the Cabinet, a Supreme Court Justice, or an "internationally protected person." (18 USC §§ 351, 1116, 1751).

(b) To assist the Department of Justice in enforcing 18 USC § 831, dealing with prohibited transactions involving nuclear materials. This statute specifically authorizes the use of DOD assets to conduct arrests and searches and seizures with respect to violations of the statute in cases of "emergency," as defined by the statute.

(c) 18 USC § 382 allows the Department of Defense to assist the Department of Justice in enforcing 18 USC § 175 & 2332, during an emergency situation involving chemical or biological WMD. DOD support in WMD situations also appears in 50 USC §§ 2311- 2367, Weapons of Mass Destruction Act of 1996. These statutes specifically authorize the use of DOD assets and in **very limited** situations provide authorization for the Department of Defense to arrest, search and seize.

b. Although statutory exceptions allow the use of military forces in some contexts, priot to committing their forces for these purposes, commanders shall consult with their judge advocates and refer to applicable DOD and Service Directives, including DODD 3025.1, *Military Support to Civil Authorities (MSCA),"* DODD 3025, *Military Assistance for Civil Disturbances (MACDIS),"* DODD 3015.15, *Military Assistance to Civil Authorities*, and DODD 5525.2 *DOD Cooperation with Civilian Law Enforcement Officials."*

~~b. Vicarious Liability. Commanders at all echelons should be aware of the legal principle of vicarious liability in planning and implementing antiterrorist measures. This principle imposes indirect Legal responsibility upon commanders for the acts of subordinates or agents. For example, willful failure on the part of the commander or a subordinate to maintain a trained and ready reaction force as required by regulation, could be construed as an act taking the commander out of the protected position found in being an employee of the Federal Government; thus making the commander subject to a civil suit by any hostages injured. Civil or criminal personal liability may result from unlawful acts, negligence, or failure to comply with statutory guidance by subordinates or agents. With the increasing number of civilian contract personnel on military installations and the sophistication of terrorist organizations, commanders should pay particular attention to meeting regulatory requirements and operating within the scope of their authority. The legal principle of vicarious liability, long established in the civilian community, has only recently applied to the military community. In this right, the command legal adviser has become increasingly important to the commander in planning, training and operational phases of the antiterrorist program.~~

~~**3. Jurisdiction and Authority for Handling Terrorist Incidents**~~

~~a. Jurisdictional Status of Federal Property in the United States, its Territories, and its Possessions. In determining whether a Federal or State law is violated, it is necessary to look not only to the substance of the offense but to where the offense occurs. In many cases, the location of the offense will determine whether the State or Federal Government will have jurisdiction to investigate and prosecute violations. There are four categories of Federal territorial jurisdiction: exclusive, concurrent, partial, and proprietary. These are shown in Figure IV-2 and discussed below:~~

Figure IV-2. Federal Territorial Jurisdiction Categories

(1) Exclusive jurisdiction means that the Federal Government has received, by whatever method, all of the authority of the state, with no reservations made to the State except the right to serve criminal and civil process. In territory that is under the exclusive jurisdiction of the United States, a State has no authority to investigate or prosecute violations of state law. However, the Assimilative Crimes Act (18 USC 13) allows the Federal Government to investigate and prosecute violations of state law that occur within the special maritime and territorial jurisdiction of the United States.

(2) Concurrent jurisdiction means that the Federal Government and the State each have the right to exercise the same authority over the land, including the right to prosecute for crimes. In territory that is under the concurrent jurisdiction of the United States and a State, both sovereigns have the authority to investigate or prosecute violations of Federal their respective laws. In addition, the Federal Government may prosecute violations of State law under the Assimilative Crimes Act.

(3) Partial jurisdiction refers to territory where the Federal Government exercises some authority, and the State exercises some authority beyond the right to serve criminal and civil process, usually the right to tax private parties. In territory that is under the partial jurisdiction of the United States, a State has no authority to investigate or prosecute violations of State law, unless that authority is expressly reserved. The Federal Government may, however, prosecute violations of state law under the Assimilative Crimes Act.

(4) Proprietary jurisdiction means that the Federal Government has acquired an interest in, or title to, property but has no legislative jurisdiction over it. In territory that is under the proprietary jurisdiction of the United States, the United States

~~has the authority to investigate and prosecute non-territory-based Federal offenses committed on such property, such as assault on a Federal officer. This authority does not extend to investigations and prosecution of violations of State laws under the Assimilative Crimes Act and Federal Crimes Act of 1970. The State has the authority to investigate and prosecute violations of State law that occur on such territory.~~

~~b. Federal Authority in the United States, its Territories, and its Possessions. Several Federal criminal statutes apply to terrorist activities committed in the US or against US nationals or interests abroad. Some deal with conduct that is peculiar to terrorism, and others prescribe conduct that is criminal for anyone but in which a terrorist may engage to accomplish his or her purposes. The Assimilative Crimes Act will allow the Federal Government to investigate and prosecute violations of State law regarding terrorist acts or threats that occur within the exclusive, concurrent, or partial jurisdiction of the United States, thereby giving the Federal Government investigative and prosecutorial jurisdiction over a wide range of criminal acts. Once a violation of Federal law occurs, the investigative and law enforcement resources of the FBI and other Federal enforcement agencies become available, and prosecution for the offense may proceed through the Office of the United States Attorney General.~~

~~c. Federal and State Concurrent Authority. In some cases, terrorist acts may be violations of State law as well as Federal law. In this situation, both State and Federal enforcement authorities have power under their respective criminal codes to investigate the offense and to institute criminal proceedings. If a terrorist act is a violation of both Federal and State law, then the Federal Government can either act or defer to the State authorities depending on the nature of the incident and the capabilities of local authorities. Even where the Federal Government defers to State authorities, it can provide law enforcement assistance and support to local authorities on request. The choice between Federal or State action is made by the prosecuting authority. However, successive prosecutions are possible even where Federal and State law proscribe essentially the same offense, without contravening the Fifth Amendment prohibition against double jeopardy. Two relevant factors regarding law enforcement responsibility for a given incident are:~~

~~(1) The capability and willingness of State or Federal authorities to act.~~

~~(2) The importance of the State or Federal interest sought to be protected under the criminal statute.~~

~~d. Jurisdictional Authority. The matrix in Appendix J, "Jurisdictional Authority for Handling Terrorist Incidents," provides a summary of FBI, host-nation, and commanding officer authority and jurisdiction in investigating or resolving terrorist incidents.~~

43. Federal Agencies and the Military.

DOD forces and installations are subject to the DOD FPCON System, which is similar

in structure to the HSAS, but based on slightly different criteria for substantially different target. Knowledge of HSAS is beneficial in coordinating with civilian authorities.

a. Overview. The primary Federal organizations dealing with terrorism management are the National Security Council (NSC), Homeland Security Council (HSC), DOS, DOJ, and the Department of Homeland Security (DHS).

b. The National Security Council

(1) The NSC formulates US policy for the President on terrorist threats that endanger US interests.

(2) NSC's Counterterrorism & National Preparedness Policy Coordination Committee (PCC). This committee is comprised of representatives from State, Justice, Department of Defense, Chairman, Joint Chiefs of Staff, CIA, and FBI. The PCC has four standing subordinate groups to coordinate policy on specific areas relating to responding to terrorism. When the NSC is advised of the threat of a terrorist incident or actual event, the appropriate subordinate group will convene to formulate recommendations for the Counterterrorism and Preparedness PCC, who in turn will provide policy analysis for the Deputies Committee. The Deputies Committee then ensures that the issues brought before the Principals Committee and NSC are properly analyzed and prepared for a decision by the President.

c. Department of Justice.

(1) The DOJ is responsible for overseeing the Federal response to acts of terrorism within the United States. The US Attorney General, through an appointed Deputy Attorney General, makes major policy decisions and legal judgments related to each terrorist incident as it occurs. In domestic terrorism incidents the Attorney General will have authorization to direct an FBI-led Domestic Emergency Support Team (DEST), an ad hoc collection of interagency experts.

(2) Federal Bureau of Investigation. The FBI has been designated the primary operational agency for the management of terrorist incidents occurring within the US. When a terrorist incident occurs, the lead official is generally the Special Agent in Charge (SAC) of the field office nearest the incident under supervision of the Director of the FBI. The FBI maintains liaison at each governor's office. Because of the presence of concurrent jurisdiction in many cases, the FBI cooperates with State and local law enforcement authorities on a continuing basis. In accordance with the Atomic Energy Act of 1954, the FBI is the agency responsible for investigating a threat involving the misuse of a nuclear weapon, special nuclear material, or dangerous radioactive material. For an emergency involving terrorism or terrorist acts involving chemical or biological weapons of mass destruction the FBI also has the lead. In these efforts, the FBI coordinates with the Department of Energy, the Department of Defense, the Nuclear Regulatory Commission, and the Environmental Protection Agency, as well as several States that have established nuclear, chemical, & biological and/or weapons of mass

destruction threat emergency response plans.

d. Department of State

(1) The DOS is the lead agency for responses to terrorism occurring outside the United States, other than incidents on US flag vessels in international waters. ~~The exception to this is on the Arabian Peninsula where the DOS and DOD signed an MOU transferring responsibility for terrorism against US interests there to the Department of Defense.~~ Once military force is directed, the President and SecDef exercise control of the US military force.

(2) The Department of State has available worldwide a $5 million reward program to encourage vigilance and the reporting of possible terrorist actions. Information on this program can be obtained through the Rewards for Justice web site: http://www.rewardsforjustice.net/.

Department of State embassies have the primary responsibility for dealing with terrorism against Americans abroad.

e. Department of Homeland Security

(1) The Department of Homeland Security leads the comprehensive and unified effort to defend the nation against terrorism through analyzing threats; guarding our borders and airports; safeguarding critical infrastructure, and coordinating the response of our nation to future emergencies. Its strategic objectives in order of priority are to:

(a) Prevent terrorist attacks within the United States;

(b) Reduce America's vulnerability to terrorism; and

(c) Minimize the damage and recover from attacks that do occur.

(2) DHS is responsible for assessing the vulnerabilities to threats against the nation's critical infrastructure, including:

(a) Agriculture

(b) Food

(c) Water

(d) Public Health

(e) Emergency Services

(f) Government

(g) Defense Industrial Base

(h) Information and Telecommunications

(i) Energy

(j) Transportation

(k) Banking and Finance

(l) Chemical Industry

(m) Postal and Shipping

(3) The Department of Homeland Security merges under one roof the capability to anticipate, preempt, and deter threats whenever possible, and the ability to respond quickly when such threats do materialize by taking the lead in coordinating with other federal, state, local, and private entities to ensure the most effective response.

~~(4) DHS maintains a Homeland Security Advisory System (HSAS) to provide a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to Federal, State, and local authorities and to the American people. This system is binding on the executive branch and voluntary to other levels of government and the private sector. It provides warnings in the form of a set of graduated threat conditions that increase as the risk of the threat increases. At each threat condition, Federal departments and agencies implement a corresponding set of protective measures to further reduce vulnerability or increase response capability during a period of heightened alert. There are five threat conditions, each identified by a description and corresponding color. From lowest to highest, the levels and colors are:~~

~~(a) Low = Green. This condition is declared when there is a low~~

risk of terrorist attacks. Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures they develop and implement:

1. Refining and exercising as appropriate preplanned Protective Measures;

2. Ensuring personnel receive proper training on the Homeland Security Advisory System and specific preplanned department or agency Protective Measures; and

3. Institutionalizing a process to assure that all facilities and regulated sectors are regularly assessed for vulnerabilities to terrorist attacks, and all reasonable measures are taken to mitigate these vulnerabilities.

(b) Guarded = Blue. This condition is declared when there is a general risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Condition, Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement:

1. Checking communications with designated emergency response or command locations;

2. Reviewing and updating emergency response procedures; and

3. Providing the public with any information that would strengthen its ability to act appropriately.

(c) Elevated = Yellow. An Elevated Condition is declared when there is a significant risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Conditions, Federal departments and agencies should consider the following general measures in addition to the Protective Measures that they will develop and implement:

1. Increasing surveillance of critical locations;

2. Coordinating emergency plans as appropriate with nearby jurisdictions;

3. Assessing whether the precise characteristics of the threat require the further refinement of preplanned Protective Measures; and

4. Implementing, as appropriate, contingency and emergency response plans.

(d) High = Orange. A High Condition is declared when there is a high risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Conditions, Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement:

1. Coordinating necessary security efforts with Federal, State, and local law enforcement agencies or any National Guard or other appropriate armed forces organizations;

2. Taking additional precautions at public events and possibly considering alternative venues or even cancellation;

3. Preparing to execute contingency procedures, such as moving to an alternate site or dispersing their workforce; and

4. Restricting threatened facility access to essential personnel only.

(e) Severe = Red. A Severe Condition reflects a severe risk of terrorist attacks. Under most circumstances, the Protective Measures for a Severe Condition are not intended to be sustained for substantial periods of time. In addition to the Protective Measures in the previous Threat Conditions, Federal departments and agencies also should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement:

1. Increasing or redirecting personnel to address critical emergency needs;

~~2. Assigning emergency response personnel and pre-positioning and mobilizing specially trained teams or resources;~~

~~3. Monitoring, redirecting, or constraining transportation systems; and~~

~~4. Closing public and government facilities.~~

(~~5~~4) The United States Coast Guard

(a) ~~The Commandant of the United States Coast Guard reports directly to the Secretary of Homeland Security. However, the USCG also works closely with the Under Secretary of Border and Transportation Security as well as maintain its existing independent identity as a Military Service. Upon declaration of war or when the President so directs, the Coast Guard would operate as an element of the Department of Defense, consistent with existing law.~~ The Commandant of the United States Coast Guard reports directly to the Secretary of the Department of Homeland Security (DHS). Under DHS, the USCG maintains its statutory status as one of the five Armed Forces and conducts national security missions as a Military Service at all times. Upon declaration of war by the Congress **or** when the President so directs (may be via the convenience of any Executive Order) at any time, the USCG may be transferred to the Department of Navy, consistent with United States Code. As Service Chirf, the Commandant would report directly to the Secretary of Navy. Importantly, all law enforcement authorities of the USCG would transfer to the Secretary of the Navy, a civilian official. In addition, *posse comitatus* still would not apply to the USCG. Memoranda of Agreement with DOD exist for USCG support of Maritime Homeland Defense and the employment of USCG capabilities and resources anywhere in the world in support of the National Military Strategy.

(b) The USCG is the LFA for Maritime Homeland Security ~~and for Maritime Homeland Defense.~~ And, as such, since the Coast Guard is simultaneously and at all times both an armed force of the United States (14 USC 1), and a law enforcement agency (14 USC 89), and because terrorism can be classified as either a criminal act or an act of war, the USCG's capabilities are extremely relevant, valuable, and needed whether the threat is termed a military or terrorist attack. The Coast Guard's homeland security mission is to protect the US Maritime Domain and the US ~~Marine~~ Maritime Transportation System and deny their use and exploitation by terrorists as a means for attacks on US territory, population, and critical infrastructure. Additionally, the USCG ~~Coast Guard~~ will prepare for and, in the event of attack, conduct emergency response operations. And, when directed, as the supported or supporting commander, the Coast Guard will conduct military homeland defense operations in its traditional role as a Military Service.

(6) Federal Emergency Management Agency. As the lead agency for

consequence management, FEMA will manage and coordinate any Federal consequence management response in support of State and local governments in accordance with its statutory authorities. Additionally, FEMA will designate appropriate liaison and advisory personnel for the FBI's Strategic Information and Operations Center and deployment with the DEST, the Joint Operations Center, and the Joint Information Center.

f. Department of Energy. The DOE will provide scientific-technical personnel and equipment in support of the LFA during all aspects of a nuclear / radiological WMD terrorist incident.

g. Department of Transportation. DOT and/or the FAA are the federal agencies responsible for responding to terrorist incidents on aircraft in flight within US jurisdiction. The FAA has exclusive responsibility in instances of air piracy for the coordination of law enforcement responses. The FBI maintains procedures, in coordination with DOS and DOT, to ensure efficient resolution of terrorist hijackings.

h. Department of the Treasury

(1) The Department of the Treasury is responsible for preventing unlawful traffic in firearms and explosives, and ~~by~~ for protecting the President and other officials ~~form~~ from terrorist attacks.

(2) The Department of the Treasury, in cooperation with the Department of State Rewards Program, has also launched a Counter-Terrorist Financing Rewards Program for information leading to the dismantling of any system used to finance a terrorist organization and for information leading to the arrest or conviction of those who planned or aided in any act of terrorism against US persons or property. Information about individuals or organizations that finance terrorists can be submitted ~~by calling **1-866-867-8300** within the US or~~ by contacting the nearest US embassy or consulate if outside the US.

i. Director, Central Intelligence. The DCI is the lead in the Intelligence Community for reducing vulnerabilities through aggressive foreign intelligence collection, analysis, counterintelligence, and covert action in accordance with the National Security Act of 1947 and EO 12333, UNITED STATES INTELLIGENCE ACTIVITIES, 4 December 1981.

j. The Environmental Protection Agency (EPA). The EPA will provide technical personnel and supporting equipment to the LFA during all aspects of a WMD terrorist incident.

k. The Department of Health and Human Services (DHHS). DHHS is the primary agency to plan and to prepare for a national response to medical emergencies arising from the terrorist use of WMD. DHHS provides technical personnel and supporting equipment to the LFA during all aspects of a terrorist incident.

l. Department of Defense

(1) US Armed forces are prepared, on order, to attack terrorists or states involved in sponsoring terrorism. DOD Directive 2000.12, *D~~e~~OD Antiterrorism Program*, now prescribes that the ASD-(SO/LIC) has the lead role within the Department of Defense in countering domestic terrorist incidents where US forces may be used. The military is to maintain at least one domestic terrorism rapid response team composed of members of the Armed Forces and employees of the Department of Defense with the appropriate expertise. Active duty, National Guard, and Reserve forces possess expertise, training, and equipment that can support responses to chemical, biological, and radiological attacks at DOD installations and civilian communities. Expert and capable technical organizations and tactical units such as EOD teams, WMD CST teams, the Marine Corps Chemical Biological Incident Response Force, and the Army's Technical Escort Unit are involved in the development of response plans and procedures. These units can assist the FBI on-site in dealing with chemical and biological incidents, such as identification of contaminants, sample collection and analysis, limited decontamination, medical diagnosis and treatment of casualties and render safe procedure for WMD devices. JDOMS will serve as the executive agent for all domestic consequence support. However, the Attorney General, through the FBI, will remain responsible for coordinating:

(a) The activities of all Federal agencies assisting in the resolution of the incident and in the administration of justice in the affected areas.

(b) These activities with those state and local agencies similarly engaged. For the military planner in the United States, its territories and possessions, this relationship between DOJ and the Department of Defense requires the development of local memorandums of agreement or understanding, between the installation, base, unit, or port, and the appropriate local FBI office. This precludes confusion in the event of an incident. These local agreements, because of military turnover and reorganization, should be reviewed and tested annually. When updates or new MOUs/MOAs are accomplished coordinate with ASD(HD), as required.

(2) It is DOD policy that:

(a) The commanders at all levels have the responsibility and authority to enforce appropriate security measures to ensure the protection of DOD elements and personnel subject to their control and shall ensure the AT awareness and readiness of all DOD elements and personnel (including dependent family members) assigned or attached. Commanders must ensure appropriate AT protection and readiness of DOD elements and personnel while pursuing mission accomplishment.

(b) The geographic combatant commanders' AT policies take precedence over all AT policies or programs of any DOD Component operating or existing in that command's AOR except for those under the security responsibility of a COM. All DOD ~~P~~personnel traveling into a combatant commander's AOR will

familiarize themselves with all AOR-specific AT policies and comply.

(c) All DOD military, DOD civilians, DOD dependent family members, and DOD contractors shall comply with theater, country, and special clearance requirements before overseas travel.

(d) The commanders do not have the same legal responsibility to provide security for DOD contractors as that provided for military forces or direct-hire employees. Contractors remain private US citizens. The Department of Defense shall assist the Department of State (DOS), where militarily feasible, in supporting efforts to protect US citizens abroad. Contractors are required to contact the combatant command to obtain, and comply with, the specific AT guidance for that particular area. Commanders are required to offer AT training to contractors under the terms specified in the contract. Contractors working within a US military facility or in close proximity of US Forces shall receive incidentally the benefits of measures undertaken to protect US Forces.

(e) Compliance with the "No Double Standard" policy on dissemination of terrorist threat information is maintained.

"No Double Standard Policy"

It is the policy of the ~~U.S.~~US Government that no double standard shall exist regarding the availability of terrorist threat information and that terrorist threat information be disseminated as widely as possible. Officials of the ~~U.S.~~US Government shall ensure that information that might equally apply to the public is readily available to the public. The Department of Homeland Security (DHS) is responsible for the release of information to the public in the 50 United States, its Territories, and Possessions. The Department of State (DoS) is responsible for release of terrorist threat information to the public in foreign countries and areas. Threats directed against or affecting the public (in the 50 United States, its Territories, and Possessions) or ~~U.S.~~US citizens abroad shall be coordinated with the DHS, the DoS, or the appropriate ~~U.S.~~US Embassy before release.

Commanders may disseminate terrorist threat information immediately to D~~o~~OD Elements and Personnel for threats directed solely against the Department of Defense. In foreign countries and areas, the threat information also shall be passed up the chain of command to the lowest level that has direct liaison with the DoS or the appropriate ~~U.S.~~US Embassy(ies) (or for non-Combatant Commander assigned forces, the ~~U.S.~~US Defense Representative (USDR)). Within the 50 United States, its Territories, and Possessions, the threat information shall be passed up the chain of command to the lowest level that has direct liaison with the DHS. Except when immediate notice is critical to the security of D~~o~~OD Elements and Personnel, the appropriate DoS/~~U.S.~~US Embassy(ies)/DHS should be informed of the threat information before release to ~~DoD~~ DOD Elements and Personnel. When immediate notice is critical to the security of D~~o~~OD Elements and Personnel, Commanders may immediately disseminate the information to, and implement appropriate AT protective measures for, D~~o~~OD Elements and Personnel; and as soon as possible, inform the DoS/~~U.S.~~US Embassies or the DHS, as appropriate, through the chain of command.

Commanders also shall inform the DoS/~~U.S.~~US Embassy(ies) or the DHS of any changes to FPCON Levels or the security posture that significantly affects the host

nation/~~U.S.~~US public. When FPCONs are changed based upon received threat information, both the threat information and notice of the changed FPCON shall be passed up the chain of command to the lowest level that has direct liaison with the DoS/~~U.S.~~US Embassy(ies) (or for non-Combatant Command assigned forces, the USDR) or the DHS. Coordination and cooperation with the DoS/~~U.S.~~US Embassy or the DHS in these cases is NOT a request for concurrence. Rather, it is informing the COM or Secretary of Homeland Security of the D~~o~~OD response to a given terrorist threat. Although the COM or Secretary of Homeland Security may not agree with the commander's assessment, the ultimate responsibility for protection of D~~o~~OD Elements and Personnel rests with the commanders in the chain of command. In areas outside the purview of the DHS, the DoS is responsible to determine whether to release the threat information to ~~U.S.~~US citizens abroad and to deal with the sensitivities of the host nation(s). In the areas under the *purview of the DHS, the Secretary of Homeland Security is responsible to determine whether to release the threat information to the ~~U.S.~~US public.*

DODD 2000.12, *D~~o~~OD Antiterrorism (AT) Program*

(3) The Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict, under the Under Secretary of Defense for Policy (USD[P]), shall serve as the Principal Staff Assistant and civilian advisor to the USD(P) and the Secretary of Defense to provide overall direction and supervision for policy, program planning and execution, and allocation of resources for the AT activities of the Department of Defense.

(4) Antiterrorism Coordinating Committee Senior Steering Group (ATCC-SSG). All Federal Agencies are required to take all steps necessary to reduce vulnerabilities to terrorist attacks. The ATCC and ATCC-SSG were established to meet this requirement and to support the Secretary of Defense and the Chairman of the Joint Chiefs of Staff in fostering cooperation and coordination for AT activities within the Department of Defense and among the Department of Defense and other US Government Agencies and organizations.

(5) Military Authority. See Figure IV-2.

Figure IV-3. Approval for Use of Military Force

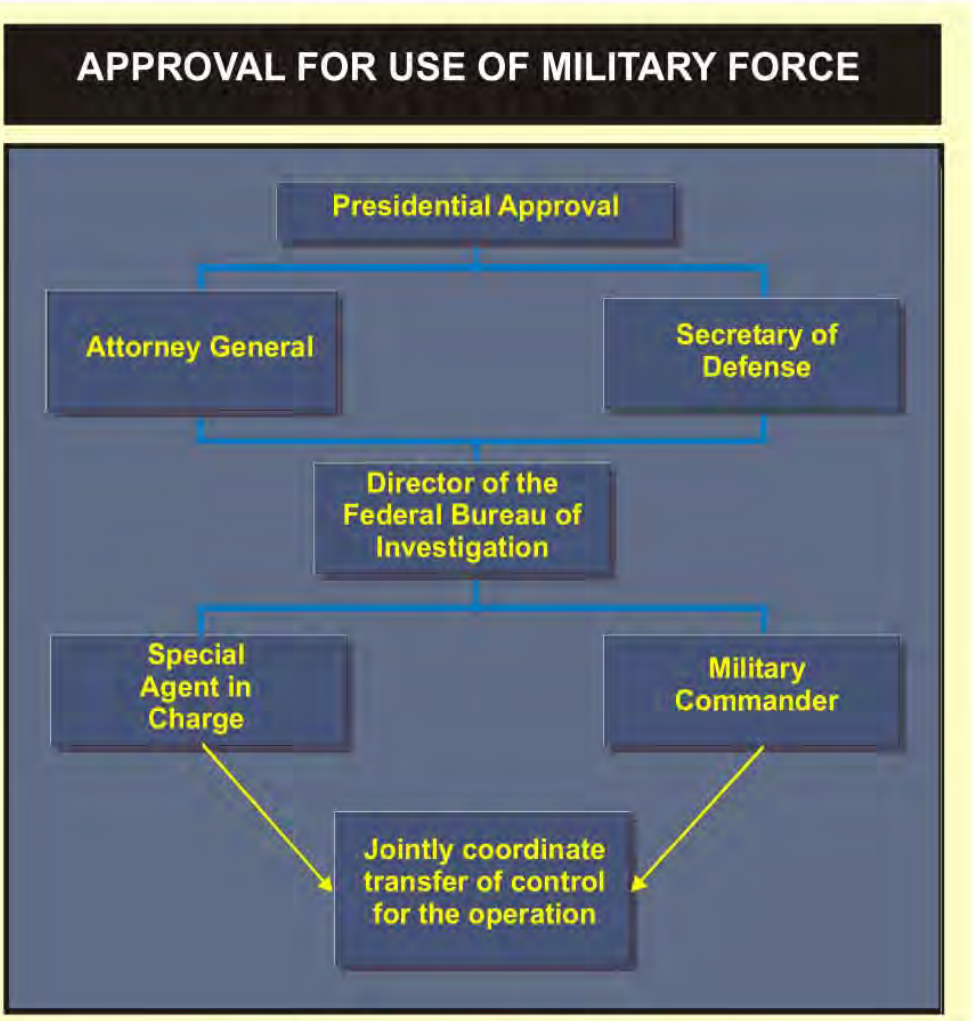

Figure IV-2. Approval for Use of Military Force

(a) Upon notification of Presidential approval to use military force, the Attorney General will advise the Director of the FBI, who will notify the SAC at the terrorist incident scene. The Attorney General will also notify the Secretary of Defense, who will advise the military commander. The military commander and the SAC will coordinate the transfer of operational control to the military commander. Responsibility for the tactical phase of the operation is transferred to military authority when the SAC relinquishes command and control of the operation and it is accepted by the on-site military commander. However, the SAC may revoke the military force commitment at any time before the assault phase if the SAC determines that military intervention is no longer required and the military commander agrees that a withdrawal can be accomplished without seriously endangering the safety of military personnel or others involved in the operation. When the military commander determines that the

operation is complete and military personnel are no longer in danger, command and control will be promptly returned to the SAC.

(b) For ~~the military planner~~ planning within ~~in~~ the United States, its territories, and its possessions, this relationship between the DOJ and Department of Defense requires the development of local memorandums of agreement or understanding between the installation, base, unit, or port and the appropriate local FBI office to preclude confusion in the event of an incident. Because of military turnover and reorganization, these local agreements should be reviewed and tested annually.

4. Military Installation Commander's Responsibilities.

PDD-39 directs federal agencies to ensure that the people and facilities under their jurisdiction are protected against terrorism. This applies to DOD facilities both abroad and in the US.

a. Domestic Incidents. Although the FBI has primary law enforcement responsibility for terrorist incidents in the United States (including its possessions and territories), installation commanders are responsible for maintaining law and order on military installations. Plans should address the use of security forces to isolate, contain, and neutralize a terrorist incident within the capability of installation resources. In the United States, installation commanders will provide the initial and immediate response to any incident occurring on military installations to isolate and contain the incident under the direction of Commander, US Northern Command (USNORTHCOM). The FBI takes the following steps:

(1) The senior FBI official will establish liaison with the command center at the installation. If the FBI assumes jurisdiction, the FBI official will coordinate the use of FBI assets to assist in resolving the situation (e.g., hostage rescue team, public affairs assets).

(2) If the FBI assumes jurisdiction, the Attorney General will assume primary responsibility for coordinating the Federal law enforcement response.

(3) If the FBI declines jurisdiction, ~~the senior military e~~Commander, USNORTHCOM, as the Geographic Combatant Commander, will take action to resolve the incident.

(4) Even if the FBI assumes jurisdiction, the military commander will take immediate actions as dictated by the situation to prevent loss of life or to mitigate property damage before the FBI response force arrives.

(5) In all cases, command of military elements remains within military ~~e~~Channels under the direction of Commander, USNORTHCOM.

(6) Response plans with the FBI and Service agencies should be

exercised annually at the installation and base level to ensure that the plans remain appropriate.

b. Foreign Incidents.

(1) For foreign incidents, the ~~installation~~ unit commander's responsibilities are the same as for domestic incidents — with the added requirement to notify the HN and DOS. Notification to the DOS is made at the geographic combatant commander level. In all theaters, existing plans provide guidance to the installation commander regarding notification procedures. DOS has the primary responsibility for dealing with terrorism involving Americans abroad. The installation's response is also subject to agreements established with the HN. Such agreements, notwithstanding, the *Standing Rules of Engagement* (CJCS Instruction 3121.01A), make it clear that the commander retains the inherent right and obligation of self-defense ~~even in such situations~~. In addition, under standing rules of engagement, the inherent right of self-defense still applies in situations off base in foreign areas. If US forces (or members thereof) are actually under attack, they retain the inherent right to respond with proportionate, necessary force until the threat is neutralized. This is providing that the host nation is unwilling or unable to respond to the threat in sufficient time or with the appropriate means.

(2) The response to off-installation foreign incidents is the sole responsibility of the HN. US military assistance, if any, depends on the applicable SOFA or MOU and is coordinated through the US Embassy in that country. Military forces will not be provided to host-nation authorities without a directive from the Department of Defense that has been coordinated with the DOS. The degree of DOS interest and the involvement of US military forces depend on the incident site, nature of the incident, extent of foreign government involvement, and the overall threat to US security.

c. AT plans will:

(1) Be implemented by combatant commands, subunified commands, JTFs, and component commands, IAW responsibilities and procedures established in DODD 2000.12, *D~~o~~OD Antiterrorism (AT) Program*, DODI 2000.14, *D~~o~~OD Combating Terrorism Program Procedures*, DODI O-2000.16, D~~o~~OD ~~Combating Terrorism Program~~ Antiterrorism Standards, and DOD 2000.12-H, "Protection of DOD Personnel and Activities Against Acts of Terrorism and Political Turbulence"; *D~~o~~OD Antiterrorism Handbook*.~~;~~

(2) Be coordinated with and approved by the combatant commander or a designated representative;

(3) Address the use of installation security forces, other military forces, and host-nation resources (In many situations through agreement with host-nation authorities, the plan will probably evolve into the installation having responsibility "inside the wire or installation perimeter" and the HN having responsibility "outside the

wire or installation perimeter." The wide dispersal of work areas, housing, support [medical, child care, exchange, morale, welfare, and recreation], and utility nodes [power grids, water plants] may require US responsibility for certain fixed-site security outside the wire. This could be accomplished by a quick reaction force);

(4) Be coordinated by the combatant commander with both host-nation and DOS officials; and

(5) Be exercised annually with host-nation resources to ensure that the plan remains appropriate.

d. Although the installation commander may not have security responsibility "outside the wire," he still maintains a security interest. The installation commander must include exterior terrain, avenues of approach, threat capabilities (possession of stand-off weapons such as MANPADs or mortars), hazardous material storage in proximity to the US Forces, and host nation security processes when developing security plans for the installation, regardless of who provides exterior defense.

CHAPTER V
ANTITERRORISM PROGRAM; INSTALLATION, BASE, SHIP, UNIT, AND PORT

"Night and day we chased an enemy who never awaited our approach but to harm us, was never found sleeping. Each tree, each hole, each piece of rock hid from our unseeing eyes a cowardly assassin, who, if undiscovered, came to pierce our breasts; but who fled or begged for mercy if we found him face to face."

Unknown Creole during the Haitian War for Independence, 1793

1. Overview of Program Concept

To meet the terrorist threat, an integrated and comprehensive AT program must be developed and implemented at every echelon of command. The program ~~is designed~~ applies a wartime defensive mindset to foster a protective posture in peacetime (i.e., units performing normal duties and serving in security assistance organizations, peacekeeping missions, or mobile training teams) ~~that will carry over to a wartime environment~~. ~~Antiterrorist measures are intended to identify and reduce the risk of loss or damage of potential targets and to develop procedures to detect and deter planned terrorist actions before they take place, thereby reducing the probability of a terrorist event. The measures also encompass the reactive or tactical stage of an incident, including direct contact with terrorists to end the incident with minimum loss of life and property.~~ Antiterrorism programs should be incorporated and ~~integrated~~ coordinated with DODD 3020, Defense *Critical Infrastructure Protection,* planning, coordination, community cooperation, and synchronization, which is required for every Service, installation, base, ship, unit, and port.

a. Command and Control. When terrorists attack DOD property or personnel, the National Military Command Center becomes the operations center for the Joint Staff and the Secretary of Defense. The incident command, control, and reporting responsibilities for ~~foreign~~ terrorist attacks on DOD property or personnel belong to the geographic combatant commander within whose AOR the attack has occurred. For assets under the control of a functional combatant commander (e.g., Commander, United States Special Operations Command) the functional combatant commander will coordinate with the affected geographic combatant commander for an appropriate division of responsibilities. Combatant command reporting will use the National Military Command System. ~~Domestic terrorist attacks on DOD property or personnel will be reported by the Service or agency in command of the targeted installation.~~

b. AT Program Elements. The AT program stresses deterrence of terrorist incidents through preventive measures common to all combatant commands and Services. In order to be successful, an AT program must be implemented in a methodical, coordinated manner. ~~Although an installation or unit may already have some elements in place, all program areas should be reviewed thoroughly on at least an annual basis.~~ It cannot be stressed enough that the AT Program is the ultimate responsibility of the commander or, in the case of a DOD Agency, the civilian equivalent. ~~As such he or~~

~~she~~ who has the authority and responsibility to alter or add to the AT program as deemed necessary to accommodate the local situation. The AT Program elements described below are merely the minimum recommended issues that should be addressed.

(1). All the elements and assessments of the Risk Management process.

(a) Threat Assessment Standards. DOD Instruction 2000.16, *D~~o~~OD Antiterrorism Standards*, provides guidance for conducting a threat assessment.

1. Development of AT Standards.

2. Coordination in Overseas Locations.

3. Application of DOD Terrorism Threat Analysis Methodology.

4. Threat Information Collection and Analysis.

5. Threat Information Flow.

6. Potential Threat of Terrorist Use of WMD.

(b) In order to develop a site-specific ~~TA~~ threat and vulnerability assessment, Antiterrorism Officers (ATOs) should refer to Combatant Commander/Service directives. Consider using the Joint Staff J-34 Joint AT program manager's guide (JAT Guide) ~~Installation Antiterrorism Program and Planning Tool (IPT)~~ as it shall facilitate what would otherwise be an extremely time consuming process. The tool assists directly in the development of the installation's AT Plan, using pre-incident FPCON measures and post-incident response measures.

(c) Criticality/Vulnerability/Risk Assessments. Much like the threat assessment, multiple DODI 2000.16 standards address conducting vulnerability assessment and program reviews. Some standards are program centric while others focus on VAs. These standards are:

1. Comprehensive AT Program Development, Implementation, and Assessment.

2. Antiterrorism Officers (ATOs).

3. AT Program Review.

4. VAs of Installations.

5. Pre-deployment AT Vulnerability Assessment.

(2) Planning.

(a) Planning Standards. DODI 2000.16 provides guidance for the development of AT related plans. Some standards deal with the specifics of plan writing, while others address FPCON issues. FPCONs are actually a derivative of the Operations and Intelligence fusion process. The following highlighted standards affect the AT planning process:

1. Development of FPCONS.

2. FPCON Measures Implementation.

3. Threat Response Measures.

4. Comprehensive AT Program for AOR.

5. Terrorism ~~TA~~Threat and vulnerability assessment.

6. Physical Security Measures.

7. Terrorism Incident Measures.

8. Terrorist Consequence Management.

(b) Planning Integration. The JAT GUIDE, ~~J-34 Installation Planning Tool,~~ particularly Part III, provides an integrated approach to fulfilling the requirements of the above standards.

(3) Training.

(a) Training Standards. DOD Instruction 2000.16, *D~~o~~OD Antiterrorism Standards*, provides ~~guidance~~ policy for the conduct of AT-related training to include eligibility, course content for training levels I through IV (basic through flag officer), and requirements for High Risk Personnel. The individual standards are:

1. General requirements for AT Training.

2. Level I AT Awareness Training.

3. AOR Specific Training Requirements for All DOD Personnel.

4. Level II ATO Training.

5. Level III and Level IV Command & Executive

Management Training

~~5~~6. Training for High Risk Personnel and High Risk Billets.

(b) Filling In the Gaps. The DOD AT Standards give a reasonably complete picture of training requirements. The following discussion provides further analysis of the training process and the selection of a training source.

(c) Analyze Training Requirements. Training is absolutely vital to the success of any AT program. The requirements for Levels I and II training are fairly straightforward. In AT, success rests on the foundation of awareness. However, some supporting skills, and resources such as how to conduct an assessment, and SIPRNET access, constitute a hidden set of necessary training. ATOs must take an exacting look at the current inventory of skills, determine which are needed, and develop a strategy to close the gap.

1. Training Strategy Development. ~~The solution is to let your AT working group do the development work. This solution shall make use of their varied expertise as well as giving them ownership of the strategy. Instead of imposing the training externally, this approach allows for a process of internal adoption. From an organizational viewpoint, this shall greatly speed the rate at which training occurs.~~ The Commander, through the operations staff, conducts the mission analysis necessary to incorporate AT TTP into individual and collective training. The approved strategy is then outlined within the unit training guidance and training goals.

(d) Leverage AT Training and Expertise. The most obvious source of Level II trained personnel is your Service school. However, other options can be found in the toolbox. Cost and availability figure most heavily in selecting the supplier for each category. Quite often, organizations like the Interagency Operations Security (OPSEC) Support Staff ~~shall~~ can conduct mobile training teams at your location to train large numbers of individuals at a relatively low cost.

(4) Exercises.

(a) Exercise Standards. Commanders at all levels are required to exercise their AT plans at least annually.

(b) Incremental Approach. Success is often achieved through steady, incremental progress ~~(crawl before walking, walk before running)~~. With this mindset, it is wise to begin by conducting staff exercises. Although the exercise requirement is an annual one, during the initial phases of a program, you may have to conduct a separate staff exercise, a communications/logistics exercise, and a field exercise all in 1 year. Remember that AT Plans ARE NOT considered to be valid or executable until they have been exercised. However, there is no requirement to exercise AT plans in a vacuum. AT scenarios/injects can be incorporated into a larger exercise in

order to extract the maximum training benefit for all concerned.

(c) Psychological Effect. An active exercise program can create an impression of strength. Remember that people react to their perceptions as though they are reality. Terrorists are no exception. ~~If terrorists can see that the US is prepared for their attacks, they shall shift their efforts elsewhere, thus fulfilling your AT Program's goal of deterring terrorist acts.~~

(d) Identifying Shortfalls. Exercises Identify Resource Shortfalls. This presupposes a mechanism for capturing lessons learned. Once the command identifies shortfalls, the process of covering the gaps can begin. The answer ~~shall~~ is not always be an external provision of additional resources. Often, the answer ~~shall~~ may be the reprogramming of internal resources.

(e) Joint Exercises/Operations. Nearly all combat operations, ~~now and in the future, shall~~ will normally be joint operations. However, ~~U~~unless our forces practice AT procedures during joint operations to resolve interoperability issues, ~~soft spots~~ vulnerabilities ~~shall~~ will be created. Since terrorists specialize in asymmetric attacks, failure to conduct joint AT exercises is a high-risk proposition.

(5) Resource generation

DOD O-2000.12-H, *D~~o~~OD Antiterrorism Handbook*, Chapter 16, provides a detailed description of the minimum essential elements of generating resource requirements for AT Programs. AT Program reviews shall include an assessment of the following:

(a) Generating requirements.

(b) Documenting resource requirements.

(c) Prioritizing resource requirements.

(d) Funding sources.

(e) Unfunded requirement submissions.

(6) Program Reviews.

VAs support the AT program review by identifying shortfalls in the program itself. Areas to focus the assessment should include, but not be limited to, the following:

(a) AT Plans and Programs.

(b) CI, Law Enforcement Liaison, and intelligence support.

(c) AT Physical Security Measures.

(d) Vulnerability to a Threat and Terrorist Incident Response Measures.

(e) VAs for Terrorist Use of WMD.

(f) Host Nation, Local Community, Inter-Service, and Tenant Support.

c. AT Program Concept. The AT program concept represents an integrated, comprehensive approach within combatant commands and the Services to counter ~~the~~ terrorist threats to military installations, bases, ships, facilities, equipment, and personnel. ~~By definition, t~~The AT plan contains all the specific measures ~~taken~~ necessary to establish and maintain an AT program that meets the standards of DOD Directive 2000.12, *D~~o~~OD Antiterrorism (AT) Program* and DOD Instruction 2000.16, *D~~o~~OD Antiterrorism Standards*. AT program elements include all the elements and assessments of the Risk Management process, planning, training and exercises, resource generation and a comprehensive program review. ~~Accordingly, an effective AT plan accounts for all aspects of the AT program.~~

d. AT Plan Requirements

At a minimum, the AT plan must address the key elements discussed below. These elements must be integrated into and/or support a comprehensive AT program. Stand-alone documents (e.g. Standard Operating Procedures, local regulations, or operations orders that articulate requirements for these key elements) shall be replicated in and/or referenced by the AT plan. The Threat, Critically, and Vulnerability Assessments are components of a single integrated process and the risk assessment (management) process is last, so resources or the lack thereof will be assigned as the working group and Commander feels need for their specific area.

(1) Threat Assessment. The terrorism ~~TA~~ threat and vulnerability assessment is the tool that commanders use to arrive at a judgment of risk and consequences of terrorist attack. This assessment focuses on the full range of known or estimated terrorist capabilities in the commander's area of interest, including WMD. Annually, or upon FPCON change, commanders integrate threat information prepared by the intelligence, counterintelligence and law enforcement communities, technical information from security and engineering planners, and information from other sources to prepare their assessments (see Appendix A).

(2) Vulnerability Assessment. This assessment provides a vulnerability-based analysis of an activity's AT program. A tool for the commander, the VA is the process to determine the susceptibility to attack by the broad range of terrorist threats against personnel and assets. The result of the assessment provides a basis for

determining options to eliminate or mitigate vulnerabilities. Commanders shall conduct a dedicated local VA at least annually, but there should be a means to adjust the assessment as the threat changes (see Appendix B). There may be several vulnerability assessments conducted on an installation (i.e., water vulnerability, CBRN vulnerability, etc.); the finding of these functional area vulnerability assessments must be included in the overall installation assessment.

(3) Criticality Assessment. The criticality assessment shall provide the commander with a prioritized list of assets based on the necessity for mission completion (see Appendix C). Inputs from all organizations shall be required to determine what assets are required and how many. The completed information may be compiled into a criticality matrix. This information is then combined with the threat and vulnerability information to assess the AT risk.

(4) Risk Assessment. Commanders conduct a RA to integrate threat, criticality and vulnerability information in order to make conscious and informed decisions to commit resources or enact policies and procedures that mitigate or define the risk. RA provides the commander with a clear picture of the current AT posture and identifies those areas that need improvement. When conducting this assessment, commanders shall consider the threat, asset criticality, and vulnerability of facilities, programs, and systems, as well as deterrence and response capabilities.

(5) AT FPCON Measures. FPCON AT measures are the actions taken at facilities to deter and/or prevent a terrorist(s) from conducting an attack. FPCONs are the principal means through which commanders (or DOD civilian equivalent) apply an operational decision to best protect personnel or assets from terrorist attack. AT measures assimilate facilities, equipment, trained personnel, and procedures into a comprehensive effort designed to provide optimal AT protection to personnel and assets. The objective is to ensure an integrated approach to terrorist threats. Well-designed AT measures direct actions that ensure threat detection, assessment, delay, denial, and notification. AT measures should include provisions for the use of physical structures, physical security equipment, chemical-biological-nuclear-radiological-explosive detection and protection equipment, Random Antiterrorism Measures, response forces, and other emergency measures (see Appendix F). AT measures should be scalable and proportional to increases in the local threat and/or unit operational capability.

(6) Terrorist Incident Response Measures. These include procedures to provide command, control, communication, and intelligence with the first responders charged with the task of determining the full nature and scope of the incident, containing damage, and countering the terrorist(s) that may still be present. The objective of terrorist incident response measures is to limit the effects and the number of casualties resulting from a terrorist attack. These measures and the strategy that ties them together can also contribute to deterring terrorist attacks if our adversaries recognize our ability to limit the effects of their attacks.

(7) Terrorist Consequence Management ~~Measures~~ Pre-planned

Responses. Terrorist consequence management ~~measures~~ pre-planned responses should include emergency response and disaster planning and/or preparedness to recover from a terrorist attack, to include WMD. Although not an element of AT, commanders shall include terrorist consequence management preparedness and ~~response measures~~ pre-planned responses as an adjunct to the organization's AT plan. In addition, special circumstances imposed by terrorist attacks utilizing WMD shall require immediate close coordination with higher command and host nation, and/or Federal, State, and local authorities.

(8) Coverage for Off-Base Assets. In planning the coverage of off-base assets and infrastructure selected for inclusion in the facility, installation, or activity AT program, include notifications to the appropriate first responders, including law enforcement offices, and the servicing FBI field office. This shall enable integration of the facility into their response and contingency planning and provide a potential source to assist the facility in its own preparations and response. As necessary, validate and monitor the scope and viability of the coverage. If the asset is a cleared contractor facility, provide for reporting to the servicing Defense Security Service (DSS) Industrial Security Field Office (see DOD 5520.22-R, *Industrial Security Regulation*) of information that indicates classified information under facility control is or could be at risk. Promptly notify the servicing DSS office of any security requirements which the installation or activity intends that the cleared industrial facility implement.

2. AT Plan Development

a. The ~~organization's C~~commander is responsible for the development of the AT plan. The ATO is normally assigned the task of actually writing the plan. The ATO should leverage the capabilities of the organization's AT Working Group to assist in the process. Using the AT Working Group ensures the participation, input, and "buy-in" of the necessary subject matter experts and others with key responsibilities.

b. ~~There is no directed methodology for developing an AT plan.~~ The responsibility to achieve thorough integration and avoid a "stovepiped" information flow rests with the ATO. Everyone involved in developing the plan must be familiar with all applicable AT directives and instructions. DOD *Antiterrorism Force Protection Installation Planning Template* and Weapons of Mass Destruction Appendix *Antiterrorism Force Protection Installation Planning Template* (copy available from the Deputy Directorate for Antiterrorism and Homeland Defense) detail the steps necessary to produce an AT plan. A sample Antiterrorism Plan Format is also provided in Appendix D.

c. The following three phases are offered as a means to logically develop an AT plan:

(1). Phase 1: Risk Assessment. Conduct the RA only after completing the criticality, threat, and vulnerability, and criticality assessments. Any plan that does not start with these assessments shall be too reactive, misdirect resources, and result in

wasted efforts and resources.

(2). Phase 2: Build AT FPCON Measures Matrices, Terrorist Incident Response Measures Matrices and Terrorist Consequence Management Measures Matrices. This phase produces the heart of the AT plan and represents the "Concept of Operations" in the five paragraph operation order format. The end products of this phase shall be matrices of integrated pre-incident action sets to implement each FPCON security measure at the five distinct FPCONs. Each integrated action set shall identify who shall act, when they shall act, where they shall act, what the action is and the resources to be used, and how these actions shall occur at the various FPCONs. There should be similar matrices for each type of terrorist incident response and consequence management event. This section also contains detailed Physical Security measures, which are an outcome of developing the AT FPCON and Terrorist Incident matrixes.

(3) Phase 3: Writing the AT Plan. The challenge for the ATO responsible for writing the plan is to select a format that best suits the organization's ability to understand the plan, and to execute it quickly and decisively when required. While there is no mandated format, it is recommended that organizations use the format included in Appendix D ~~standard five paragraph order outlined in JP 5-002, *Joint Task Force Planning Guidance and Procedures*~~. Each level of organization shall necessarily produce an AT plan consistent with their mission and responsibilities. For example, at the installation level, the AT plan shall have a very tactical perspective and provide minute details for actions to be taken locally. A ~~geographic~~ combatant commander's plan, on the other hand, shall be at the operational level and shall provide descriptive guidance rather than prescriptive solutions.

3. Combatant Commander's Responsibility

The geographic combatant commander ~~with permanently assigned forces~~ designates a staff officer, usually in the ~~O~~operations ~~D~~directorate, law enforcement, or security section, to supervise, inspect, test, and report on the base AT programs within the theater. This staff section also coordinates with host-nation authorities and US embassies and consulates. Simultaneously, the ~~Intelligence Directorate of a joint staff (~~J-2~~), under the combatant commander's authority~~, disseminates intelligence on terrorist activities to ~~the~~ subordinate and supporting commands to ensure that the AT measures are appropriate to the threat. The manner in which the geographic combatant commander places importance on these staff functions usually has a direct affect on the AT readiness of subordinate commands.

Intentionally Blank

CHAPTER VI
PREVENTIVE MEASURES AND CONSIDERATIONS

"A general should direct his whole attention to the tranquility of his cantonments, in order that the soldier may be relieved from all anxiety, and repose in security from his fatigues."

Attributed to Frederick the Great

1. Commander's Responsibility

Preventive and protective security measures should be taken by military units and individual Service members to protect themselves and their ability to accomplish their mission during mobilization, deployment, employment, sustainment, and redeployment ~~and expeditionary~~ operations. Additionally, rest and recuperation (R&R) facilities also require close consideration. These facilities are frequently vulnerable due to their location and generally easy access. Service personnel are at risk of lowering their guard while using these R&R facilities. The installation, ~~base,~~ ship, unit, or port AT plan provides the mechanism to ensure readiness against terrorist attacks while the unit performs its tactical ~~and technical~~ mission during deployments. The degree of the protection required depends on the threat in a given location. Commanders must constantly evaluate security against the terrorist threat in order to effectively evaluate security requirements. This responsibility cannot be ignored ~~in any situation~~.

2. AT ~~Force Protection~~ in High-Threat Areas

The following are antiterrorism tactics, techniques, and procedures for high ~~risk~~ threat area missions~~; they~~ represent worst-case procedures. Security and force protection measures for forces performing security assistance, peacekeeping, mobile training teams, and ~~other small military~~ similar activities ~~can be derived from~~ are influenced by these measures.

a. Installations, Bases, Ships, and Expedition ary Sites~~, and Non-Urban Facilities~~. Forces are frequently employed for security operations or other short-term, conventional, combat-related tasks. Easily defended locations are often rare in urban areas because of building and population density or lack of proper cover and concealment and an inability to create perimeter stand-off. Political restrictions may also limit the military's ability to construct fortifications or disrupt areas~~,~~. Commanders, however, ~~but commanders~~ must take all practical means to ensure force protection and identify shortcomings to appropriate levels of command for resolution. Military planners should adapt existing structures to provide protection based on the mission, potential for attack, and ability to use surroundings effectively.

(1) Estimate of the Situation. The commander and staff should complete a thorough estimate of the situation using mission, enemy, terrain, troops, time, and political planning factors in developing a security assessment. ~~The following~~Figure VI-1 questions aid in developing an estimate of the terrorist situation:

SITUATION ESTIMATE CHECKLIST	
MISSION:	Who is being tasked?
	What is the task?
	When and where is this task to take place?
	Why are we performing this task?
ENEMY:	Who are the potential terrorists?
	What is known about the terrorists?
	— What is their agenda, capabilities?
	— Where is their support infrastructure?
	— Are they supported by the local population?
	— How can they be recognized?
	How do the terrorists receive information?
	— Have they infiltrated the installation, port, host nation military or the local law enforcement?
	How might the terrorists attack?
	— What is the potential for snipers, mortars, rockets, air or ground attacks, suicide attacks, arson, or kidnappings?
	Does your unit have routines?
	What is the potential for civil disturbances and could terrorists use or influence these disturbances in an attack?
	— Local law enforcement personnel and host and friendly nation intelligence services can be valuable sources of information.
TERRAIN:	What are the strengths and weaknesses of the installation, base, ship, port, and local surroundings?
	Are the avenues of approach above or below the water or ground?
	Are there observation areas, dead spaces, fields of fire, illumination, or no-fire areas (e.g., schools)?
	Are there tall buildings, water towers, or terrain either exterior or adjacent to the perimeter that could become critical?
	What local industries are in the area and what types of chemicals do they use?
TROOPS:	Are other US forces or equipment available?
	What local law enforcement, host nation, allied or friendly nation assets might be available?
	How do I vet non US personnel, such as contractors and other foreign or third country national who come on to the base?
	Are engineers and/or EOD in the area and will they be able to provide support?
	Are emergency reinforcements available?
	Are MWD teams available?

	What are the host-nation responsibilities, capabilities, and attitudes toward providing assistance?
	What restraints will be imposed by the USG on the show or use of force?
COMMUNICATIONS:	Is there a method for mass alerting across the base?
	What radios are used on base?
	Are they secure?
	Is there redundancy in the system?
TIME:	What is the duration of the mission?
	Are there time constraints?
	Will there be sufficient time to construct force protection facilities such as barriers, fences, and lights?
POLITICAL PLANNING FACTORS:	Are there host-nation concerns or attitudes that will impact on the situation?
	Will the situation be influenced by the existence of any religious, cultural, racial, or allied political concerns?

Figure VI-1. Situation Estimate Checklist

~~(a) Mission:~~

~~1. Who is being tasked?~~

~~2. What is the task?~~

~~3. When and where is this task to take place?~~

~~4. Why are we performing this task?~~

~~(b) Enemy:~~

~~1. Who are the potential terrorists?~~

~~2. What is known about the terrorists?~~

~~3. How do the terrorists receive information?~~

~~4. How might the terrorists attack? (Think like the terrorists! Would you ambush or raid? Would you use snipers, mortars, rockets, air or ground attacks, suicide attacks, firebombs, or bicycle, car, or truck bombs?)~~

~~5. Does your unit have routines?~~

~~6. What is the potential for civil disturbances and could terrorists use or influence these disturbances in an attack? Local law enforcement~~

personnel ~~(e.g., host-nation police) can at times be a valuable source for this information.~~, host and friendly nation intelligence services can be valuable sources of information.

~~(c) Terrain:~~

~~What are the strengths and weaknesses of the installation, base, ship, port, and local surroundings?~~

~~2. Are the avenues of approach above or below the water or ground?~~

~~3. Are there observation areas, dead spaces, fields of fire, illumination, or no-fire areas (e.g., schools)?~~

~~4. Are there tall buildings, water towers, or terrain either exterior or adjacent to the perimeter that could become critical terrain in the event of an attack?~~

~~(d) Troops:~~

~~1. Determine what is the friendly situation.~~

~~2. Are other US forces or equipment available?~~

~~3. Are engineers and/or EOD in the area? Will they be able to provide support?~~

~~4. Are emergency reinforcements available?~~

~~5. Are MWD teams available?~~

~~6. What are the host-nation responsibilities, capabilities, and attitudes toward providing assistance?~~

~~7. What restraints will be imposed by the US Government on the show or use of force?~~

~~(e) Time:~~

~~1. What is the duration of the mission?~~

~~2. Are there time constraints?~~

~~3. Will there be sufficient time to construct force protection facilities such as barriers, fences, and lights?~~

~~(f) Political Planning Factors:~~

~~1. Are there host-nation concerns or attitudes that will impact on the situation?~~

~~2. Will the situation be influenced by the existence of any religious or racial concerns?~~

(2) Develop Plan. ~~Defenses~~ Planning should include a combination of law enforcement and security assets barrier planning, ~~fortifications~~, sensors employment, other obstacles (such as ditches or barriers), local-hire security forces (if applicable), unit guards, deception, and on-call support from reaction forces. Each situation requires its own combination of abilities based on available resources and perceived need. Terrorist incident response and Terrorist consequence management planning should include considerations for fire response, NBC and TIC response (including in place sheltering and evacuation considerations), mass notification, EOD/IED response, medical response and evacuation, and mass casualty procedures.

(a) Obstacles. Obstacles slow down or disrupt vehicles and personnel approaching an area. Constructing vehicle barriers by using commercially installed electronic barriers, trenches, masonry barriers, concrete-filled oil drums, or vehicles staggered across the route creating a zigzag maze forces vehicles to slow down and make sharp turns and exposes the driver to capture or direct fire. Scattering speed bumps or sandbags on the route further slows traffic. Also consider employment of road spikes, dragon teeth, or tire shredders to slow down unauthorizes traffic. The force protection exposition and display (FPED) usually produces a compilation of useful equipment and can be found on line or requested from DTRA at atfphelp@dtra.mil. Designing entrance gates to allow access to authorized personnel while denying access to unauthorized personnel by use of controlled turnstiles provides time for observation and protection to guards and slows down direct frontal attacks. Fences, entrance gates, and obstacles should be illuminated to provide easy observation. Obstacles must be covered by observation and fire.

(b) Local Security. Local security must be around-the-clock to provide observation, early warning and, if necessary, live fire capabilities. The security should include guards at entrances to check right of entry in observation posts (OPs), around perimeter, and on rooftops to view the surrounding area. These guard positions must also be integrated into the AT plan to enable their use in augmenting responding law enforcement personnel. Security forces should have available to them

and be trained in specialized equipment for responding to terrorist attacks and/or incidents (See Figure VI-1). Local installations, with the assistance of the parent Service, should identify and procure this equipment based on Service directives and the local situation. Security review should also include review of procurement, storage, and preparation of food supplies used on base. A food vulnerability assessment can be initiated by food services personnel to review the complete food process.

(3) Establish Defense. Measures taken to establish the defense must be continually reviewed and progressively updated to counter the changing threat and add an element of unpredictability to the terrorist's calculation. Defensive measures include the

SECURITY FORCE EQUIPMENT	
Pyrotechnic pistols	Marshalling wands
Riot shotguns	Telescopes and tripods
Tear gas launchers	Binoculars
Hand-held flashlights	Night vision devices
Antiriot helmets	Loud speakers
Shields 3'6"	Fire extinguishers
Shields 6'	Cameras with flash and tripods
Side-handled or straight batons	Telescopic sights
Hand cuffs	Photographic filter
NBC protective masks	Body Armor
Handgun/rifle	Radio
Ammunition	Hearing protection

Figure VI-2. Security Force Equipment

following:

(a) Determine priority of work (assign sectors of observation and fire, construct obstacles, fortify).

(b) Improve obstacles, fortifications, and the defense as a whole. Long-term deployments should program engineer assets and force protection or physical security funds toward the construction of permanent fixtures.

(c) Establish inspections and immediate action drills, exercises, and training to implement the security plan.

(d) Maintain, when possible, secure radio or landline communications with the military police, security guards, and reaction force(s).

(e) Keep abreast of current military and host-nation police and intelligence assessments.

b. Guard Duties. Guard duties are detailed in ~~Service regulations and in local,~~ general~~,~~ and special orders and standard operating procedures. In a ~~terrorist~~ high-~~risk~~ environment, special orders should address as a minimum the following:

(1) Details of authorized passes; provide samples of passes;

(2) Procedures for searching people and vehicles;

(3) Response to approach by unauthorized personnel or hostile crowds;

(4) Specific rules of engagement (ROE) or use of force ~~policy in the event of civil disturbances, potential damage, or injury to US personnel or specific property, looting, or arson~~;

(5) Response to unauthorized photography and surveillance activities;

(6) Steps necessary to obtain police, reaction force(s), fire department, and ambulance;

(7) Guidelines for contact with host-nation police;

(8) Guidelines for contact with press and media~~;~~.

(9) Evacuation procedures.

c. Road Movement. Road movements are always vulnerable to terrorist attacks in high-risk areas. Road reconnaissance should be conducted periodically to identify high-threat areas. If possible, alternate forms of transportation (e.g., helicopters) should be used. If road movement is required:

(1) Avoid establishing a regular pattern;

(2) Vary routes and timing;

(3) Travel in groups, never single vehicles;

(4) Do not stop for dead or dying animals in/beside the road;

(5) Do not allow people to walk-up to vehicles;

(~~4~~6) Avoid traveling at night unless tactical advantage can be gained through use of night vision devices. Additional precautions should be considered if travel is required during periods of agitation (e.g., religious or political holidays);

(~~5~~7) When possible, keep a low profile (use vehicles that do not stand out);

(~~6~~8) Plan alternate routes and reactions to various threatening scenarios;

(~~7~~9) Plan communications requirements;

(~~8~~10) Avoid dangerous areas (e.g., ambush sites, areas known for violence);

(~~9~~11) Provide adequate security;

(~~10~~12) Plan in advance for maintenance and evacuation; and

(~~11~~13) Use countersurveillance.

d. Vehicle Protection. Take the following precautions when using tactical and some types of commercial vehicles, such as trucks, in a high-risk area:

(1) Place sandbags on floorboards and fenders;

(2) Cover sandbags with rubber or fiber mats;

(3) If carrying personnel, sandbag the vehicle bed as well as the driver's compartment;

(4) Remove canvas so passengers can see and shoot;

(5) Fold windshield in driver's compartment and fit high-wire cutter. Lower side windows and place wire over all openings to deflect grenades or IEDs;

(6) Normally, avoid large concentrations of personnel in any one vehicle. If necessary, assign convoys additional vehicles to disperse personnel loads;

(7) Passengers riding in truck bed face outboard and are assigned sectors of observation and fire;

(8) Rig chicken wire or chain link screens on front bumper frame to deflect rocks, bottles, firebombs, and grenades;

(9) Carry pioneer tools (fire extinguishers in particular), a line with grappling hook to clear obstacles, and tow bars for disabled vehicles;

(10) When the threat of hostile fire is constant, plan for the use of vehicles with additional armored protection.

e. Convoys. In extremely high-risk areas, consider using armed escorts for

convoy protection.

(1) Develop and rehearse immediate action drills before movement;

(2) Perform route clearance before movement;

(3) Establish and maintain communications throughout the route;

(4) Develop deception plans to conceal or change movement timing and route;

(5) If possible, include host-nation police and/or military personnel in the convoy;

(6) When selecting routes, avoid entering or remaining in dangerous areas. If ambushed, gauge response by enemy strength. Counter ambushes by accelerating through the ambush area, counterattacking, withdrawing, or withdrawing and staging a deliberate attack.

(7) Convoy escort composition depends on available forces. ~~Light armored vehicles, high mobility multipurpose wheeled vehicles, or trucks equipped with M2 50-caliber and MK19 40mm machine guns are extremely effective.~~Vehicles used should be appropriately hardened and posses the necessary weapons systems and other equipment to address the threat. Overhead helicopters and AC-130 gunships can also be used as air escorts if available. Escorts should be organized into an advance guard, main body escort, and reaction or strike group. Planning considerations are as follows:

(a) Determine concept of operation;

(b) Identify available transportation;

(c) Identify order of march and road organization;

(d) Identify disposition of advance guard, main body escort, and reserve;.

(e) Designate assembly area for convoy;

(f) Determine rendezvous time at assembly area, departure time of first and last vehicle, and expected arrival of first and last vehicle at destination;

(g) Identify action upon arrival;

(h) Determine required coordinating instructions for speed, spacing, halts, immediate action drills, breakdowns, and lost vehicles.

f. Rail Movement. Rail movement is the most difficult form of transportation to conceal and protect because it follows a predictable route and rail heads are difficult to conceal. Opportunities for deception are limited and physical security is critical. The following security precautions should be considered:

(1) Restrict passengers to military personnel only;

(2) Search for explosives or possible hijackers before departure and after every halt (MWDs are particularly suited for this mission);.

(3) Ensure that the railway is free of obstructions or explosives;

(4) Patrol the railway area;.

(5) Place armed security personnel on duty throughout the train, including engine room and trail car;

(6) Patrol and guard departure and arrival stations;

(7) Use deception measures;

(8) Provide air cover (AC-130, helicopters);

(9) Maintain communications within the train and with outside agencies;

(10) Provide reaction force to be moved by air or coordinate host-nation support (HNS) (if available).

g. Sea Movement. Sea movement, especially aboard military vessels, may provide a false sense of security. Sea operations are certainly more secure than urban patrols; however, ships in harbor or anchored off hostile coastlines are visible and high-risk targets. Crews of ships in harbors need to evaluate each new port and determine possible terrorist actions and ship's force counteractions (such as using fire and steam hoses to repel attackers). Crew members must be aware of HNS and responsibilities while in port or anchored in foreign national waters. The ship's captain is solely responsible for the ship and all those embarked. As a minimum, the captain:

(1) Establishes methods of embarkation and debarkation and patrol activities for all personnel;

(2) Identifies vital areas of the ship (for example, engine room, weapons storage, command and control bridge), and assigns security guards;

(3) Coordinates above and below waterline responsibilities;

(4) Establishes a weapons and ammunition policy and ROE, and appoints a reaction force (e.g., security alert team, backup alert force, and/or response force); and

(5) Drills all personnel involved.

h. Air Movement. For the most part, while a unit is being transported by air it is under the purview of the Air Force or air movement control personnel. Troop commanders and Air Force personnel coordinate duties and responsibilities for their mutual defense. Personnel must remain vigilant and leaders must provide adequate security. Unit security personnel coordinate with airfield security personnel, assist departures and arrivals at airfields while en route, and determine weapons and ammunition policies. Special considerations include the following topics:

(1) Road transport security when driving to and from airfields is critical. Keep arrival arrangements low profile. Do not pre-position road transport at the airport for extended periods before arrival.

(2) If pre-positioned transport is required, attach a security element and station it within the airfield perimeter. Security at the arrival airfield can be the responsibility of the HN and requires close coordination. Maintain communications between all elements until the aircraft is "wheels-up" and, upon arrival, reestablish communications with the new security element.

(3) All personnel (air crews and transported unit) must be cautioned concerning the transportation of souvenirs and other personal items that could be containers for explosives.

(4) Man-portable weapons systems in the hands of terrorists create additional planning challenges for the security of aircraft. Planning considerations should include defensive measures against such systems in the choosing of airfields and forward arming and refueling points.

i. Patrolling. Units outside the United States may be called upon to conduct patrols in urban or rural environments. These patrols will normally be planned and executed in conjunction with host-nation authorities and should be coordinated with the representatives of the appropriate staff judge advocate office and be in accordance with any applicable basing, status-of-forces, or other agreements. Patrols support police operations, expand the area of influence, gather information, police nightclubs and restaurants, detain individuals as required, conduct hasty searches, and erect hasty roadblocks. Patrols must understand the ROE. Patrolling units should avoid patterns by varying times and routes, using different exit and entry points at the base, doubling back on a route, and using vehicles to drop off and collect patrols and change areas. Base sentries or guards, other vehicle patrols, helicopters, OPs, host-nation assets, and reaction forces provide additional support.

j. Roadblocks. There are two types of roadblocks: deliberate and hasty. Deliberate roadblocks are permanent or semi-permanent roadblocks used on borders, outskirts of cities, or the edge of controlled areas. Use deliberate roadblocks to check identification and as a deterrent. Use hasty roadblocks to spot check, with or without prior intelligence. Hasty roadblocks use the element of surprise. Their maximum effect is reached within the first half hour of being positioned. Hasty roadblocks can consist of two vehicles placed diagonally across a road, a coil of barbed wire, or other portable obstacles. Roadblocks must not unnecessarily disrupt the travel of innocent civilians. Personnel manning roadblocks must know their jobs thoroughly, be polite and considerate, act quickly and methodically, use the minimum force required for the threat, and promptly relinquish suspects to civil police authorities. General principles considered in establishing roadblocks are concealment, security, construction and layout, manning, equipment, communications, and legal issues. Unless combined posts (HN and US personnel) are used, language training will be a key planning factor in employing roadblocks.

Deployed joint forces may be tasked to conduct antiterrorist operations in urban areas.

k. Observation Posts. OPs provide prolonged observation of areas, people, or buildings. OPs are critical. OPs allow observation of an area for possible terrorist activity (avenues of approach); observation of a particular building or street; ability to photograph persons or activities; ability to observe activity before, during, or after a security force operation (e.g., house search) and ability to provide covering fire for patrols. Special factors apply to OPs located in urban areas. The OP party and reaction force must know the procedure, ROE, escape routes, emergency withdrawal procedures, rallying point, casualty evacuation, and password. Cover the occupation and withdrawal of an OP by conducting normal operations (e.g., house searches, roadblocks, patrols to leave people behind), flooding an area with patrols to disguise movement, using civilian vehicles and clothes, and using deception. Any compromise of an OP location should be immediately reported.

l. Civil Disturbances. Crowd violence can either be a spontaneous emotional eruption or a planned event. In the latter case, its purpose is to draw police or troops into a target area or away from some other event. Crowd violence may also involve violence within the crowd or from opposing groups. Crowd violence is characterized by incitement and violence; both are highly contagious. Riot control aims to restore order with minimum use of force. Bearing in mind that the size or motivation of the crowd may prevent its control, the general approach is to reduce or disrupt the crowd's unifying influences and reorient the participants to concerns for personal vulnerability and welfare. The principles of riot control are shown in Figure VI-~~23~~23.

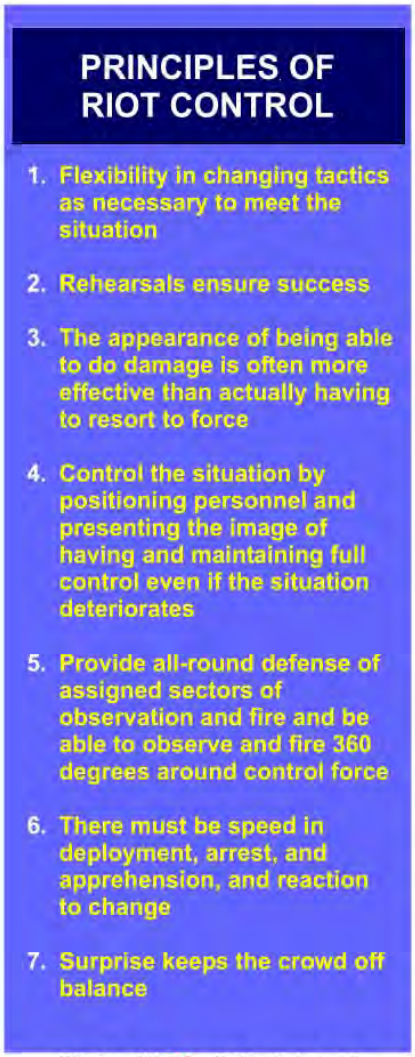

Figure VI-~~23~~23. Principles of Riot Control

m. Bomb Explosion or Discovery. The initial terrorist bomb may not be the end of the incident. The initial bomb may be designed to draw forces into an area as targets for a shooting ambush or another explosion. Upon discovery of a bomb or upon entering a bomb site, response forces should proceed with extreme caution and contact the EOD team immediately. ~~Explosive detection MWDs should be considered upon bomb discovery or during entry to the site of the explosion.~~ Explosive detection MWDs, EOD or other available detection methods should be utilized to sweep areas surrounding suspected explosive devices or incident sites for secondary devices.

n. Personal Protective Measures. Overseas deployments require a high degree of personal protective measures. DOD personnel must be aware of basic personal protective measures against terrorism, specific threats for the area they will operate in or transit, and specialized training which their duty or position requires, but the commander must also focus on the exposure of the troops to any special terrorist threat. This requires particular attention to areas where troops will live, work, and conduct R&R. Coordination between military intelligence, counterintelligence and law enforcement ~~and intelligence~~ agencies and host-nation forces is critical. The deployed military member must also understand the threat and required personal security measures.

3. Tactical Force Protection

During joint and multinational operations, US units and bases in the joint rear area (JRA) are still vulnerable to terrorist attacks. The same procedures identified in the preceding paragraphs apply. Commanders will be advised by the JRA coordinator (JRAC) of potential terrorist threats, and subordinate commands will report any terrorist activity to the JRAC. Units passing through the JRA are still required to maintain AT measures commensurate with the JRAC's guidance. Specific tactics, techniques, and procedures for operations in the JRA are contained in JP 3-10, *Joint Doctrine for Rear Area Operations*.

4. Suicide Bombers/High Risk Vehicle Checkpoints.

a. The purpose of this section is to highlight references and resources and capture best practices to enhance antiterrorism mitigation measures for conducting high risk vehicle checkpoints and deterring suicide/homicide bombers.

b. Recent vehicle borne bomb and suicide/homicide bomber attacks in Saudi Arabia and in operation IRAQI FREEDOM highlight this threat to our forces. Because of robust protective measures in place at DOD installations, our checkpoints and roadblocks are increasingly becoming prime targets for terrorists. Security forces at access control points can also be targeted as a means to gain access to installations/compounds.

c. The land component command for operation IRAQI FREEDOM and the service components have established excellent tactics, techniques, and procedures for dealing with high risk vehicle checkpoints and the suicide/homicide bomber. Tactics,

techniques, procedures and lessons learned on Service and combatant command web sites and DIA JITF-CT assessments of terrorist tactics are excellent sources for commanders and antiterrorism officers to review. The following paragraphs provide information gleaned from component threat reporting, tactics, techniques, procedures, and lessons learned.

d. Threat.

(1) Insights from recent attacks:

(a) Several vehicle bomb and suicide bomber attacks were made at checkpoints during combat operations in Iraq during March and April 2003. An Iraqi posing as a taxi cab driver feigned a break down and detonated his vehicle when four soldiers approached killing them all. Three rangers were killed in western Iraq when an SUV drove up to their check point (along with other cars) and then exploded. In another instance, an Iraqi at a checkpoint set off explosives hidden under his clothes wounding a number of marines. In all cases, deception was used to get close to US forces and increase the effect of the attack. This tactic is continuing to be used by enemy paramilitary during the stability phase.

(b) The terrorist attack on 12 May conducted against three residential housing compounds in Riyadh, Saudi Arabia occurred minutes apart using the same method. In each of these attacks, an initial assault team was used to penetrate the gate followed by another group that drove a vehicle-borne improvised explosive device through the breached gate and detonated it next to a pre-selected target on the installation. There are a number of conclusions that can be drawn from these attacks:

1. The terrorists conducted pre-operational surveillance and identified weak points at gates and in security procedures to strike soft targets and Americans.

2. The three attacks were conducted simultaneously-a signature Al-Qaeda tactic.

3. Terrorists added modifications to their tactics in order to defeat security measures that have been designed to counter previous attacks.

(2) Suicide bomber threat. All individual suicide devices are based upon the simple concept of using a human being to deliver a bomb to a target. Generally, the bomb will have the following characteristics:

(a) A simple switch for initiation consisting of a push-button or toggle switch completing an electric circuit. Relatively small initiation devices reduce the chances of discovery.

(b) Fragmentation such as nails, ball bearings, or other small

metal pieces. Dispersed fragmentation is the primary kill mechanism in individual suicide bombing attacks.

(c) Devices are generally concealed within an article of clothing worn close to the body – such as a vest, belt, or jacket. However, there have been instances where the explosive device is disguised to look like a common, innocuous object.

(d) Plasticized explosive as a main charge – usually a homemade mixture, although groups with access to greater resources utilize military grade explosives.

(e) Many devices have a backup trigger system, such as an electronic timer, pager, or booby-trap type switch. If the attacker is killed, apprehended, or attempts to abort the attack, a secondary trigger system provides an alternative initiation method.

(3) Possible indicators of a suicide/homicide bomber are as follows:

(a) An individual who deliberately ignores orders to stop or attempts to circumvent a security checkpoint.

(b) An individual wearing too much clothing for the prevailing weather conditions.

(c) A person with suspicious bulges in their clothing, carrying packages/bags, wearing satchels/backpacks or walks with unsteady gate.

(d) Individuals may exhibit a wide range of characteristics, such as clean shaven with closely cropped hair, exhibits unusual emotional demeanor such as blank stare, grin, unresponsive, and may perspire or appear gaunt and/or ill.

(e) An individual handling wires, switches, an actuator, or a dead mans switch.

(4) Vehicle borne improvised explosive device (VBIED) threat. A VBIED is a vehicle modified to conceal and deliver large quantities of explosives to a target. The motive behind such incidents is to cause many casualties and gross property damage. Possible indicators of a VBIED threat are as follows:

(a) noticeable sagging of the vehicle on its springs caused by the heavy weight of explosives found in it. Ordinarily the explosives will be placed toward the rear of the vehicle, causing it to ride lower in the rear. However, sagging springs are not normally characteristic of trucks being used for VBIEDS because these vehicles are designed to carry the weight.

(b) darkened or covered windows to conceal either the vehicles contents or the actions of the driver.

(c) unusual items inside the vehicle: gas cylinders, wires, leaflets, large bags or boxes, and batteries besides the normal car battery.

(d) Indications of a triggering device-i.e., a switch, radio transmitter, timer, wires or ropes passing from the front seat to the rear of the vehicle, etc. – visible near the driver, under the seat, or within arms reach.

(e) The presence of the vehicle in an area where it should not be, perhaps illegally parked.

(f) Holes made in the vehicle body to hide explosives and then crudely covered.

(g) Evidence that an interior door panel has been removed to hide explosives.

(h) The presence of powder or prills (small rounded granular material) left when explosive material was loaded into the vehicle.

(i) Recent painting of the vehicle to cover body alterations.

(j) additional fuel tanks, used to secrete explosives or to provide additional gasoline to fuel the explosive event.

(k) unusual smells, E.G., a burning time fuse, gasoline, fertilizer, etc.

(l) an additional antenna on the car for radio-controlled devices.

(m) any disturbance to the undercoating or dirt on the bottom of a vehicle.

(n) Indications that drivers may be associated with VBIED are the follows:

1. driving erratically; driving too slow or too fast.

2. Ignoring orders to stop, attempting to circumvent a security checkpoint, or attempting to maneuver too close to coalition assets.

3. Wearing inappropriate dress or grooming for the vehicle type.

4. Signs of nervousness, sweating, shaking, or unusual speech patterns.

5. The presence of a lone driver in the vehicle. This is standard for VBID operations; however, there could be any number of people in the vehicle if the VBIED is being driven by an unsuspecting person.

6. Inability to operate the truck or equipment properly.

7. Atypical appearance. Middle Eastern terrorists may be uncharacteristically clean-shaven and have very short haircuts. Cutting the hair is a part of the purifying ritual that many follow prior to an attack.

8. Age: mid-twenties. The average Middle Eastern suicide terrorist is about 24 or 25, but in the current Iraqi situation, age is less of a discriminator.

(o) Other suspicious conditions:

1. Occupants careful when closing the doors.

2. Vehicle left locked and unoccupied.

3. Not obviously engaged in loading or unloading.

4. Displaying hazard warning lights.

5. Parked near or adjacent to an important target.

6. Illegally parked.

(p) Common areas for concealing VBIED explosives:

1. Above roof liner.

2. Behind door panels.

3. In spare wheel well.

4. In hollowed-out seats.

5. Under false flooring.

6. Inside fuel tank (smaller alternate fuel tank elsewhere).

7. In legitimate cargo area – such as trunk, trailer, or storage bin.

8. In legitimate packaged cargo.

(q) General safe blast/fragmentation distances for VBID have been determined to be as follows:

1. Compact sedans can carry a maximum of 500 pounds (227 kilos) of explosive in the tank. This gives a lethal blast range of approximately 30 meters, and a fragmentation hazard of 381 meters.

2. Full-size sedans can carry a maximum of 1,000 pounds (455 kilos) of explosive in the tank. This gives a lethal blast range of approximately 38 meters, and a fragmentation hazard of 534 meters.

3. Passenger or cargo vans can carry a maximum of 4,000 pounds (1,818 kilos) of explosive. This gives a lethal blast range of approximately 61 meters, and a fragmentation hazard of 838 meters.

4. Small box vans (14 ft) can carry a maximum of 10,000 pounds (4,545 kilos) of explosive. This gives a lethal blast range of approximately 91 meters, and a fragmentation hazard of 1,143 meters.

5. Box van or water/fuel trucks can carry a maximum of 30,000 pounds (13,636 kilos) of explosive. This gives a lethal blast range of approximately 137 meters, and a fragmentation hazard of 1.982 meters.

6. Semi-trailer can carry a maximum of 60.000 pounds (27,273 kilos) of explosive. This gives a lethal blast range of approximately 183 meters, and a fragmentation hazard of 2,134 meters.

e. The following TTP may prove effective deterring, disarming or mitigating pedestrian suicide bomber attacks:

(1) Visual observation remains the primary method of detecting suicide bombers (see indicators in para 4.C). Screening methods can also be employed such as having suspects open their coats or lift shirts at a safe distance before approaching a checkpoint. Thermal images have proven effective for standoff detection of concealed weapons on personnel, provided that external clothing is not too heavy. These items serve as a heat sink (i.e., block radioactive emissions) and therefore are rendered as distinct spots on thermal images. This technique may prove effective for detecting concealed explosives but has not been tested in this role.

(2) If a bomber is identified, orders should be issued to evacuate the area immediately (minimum of 50 meters away) and to take cover (behind substantial

barrier). Safe distances depend upon the mass of explosive carried by the bomber and the amount and type of fragments used. Distances will necessarily be constrained in urban conditions but safety zones must be considered when selecting checkpoints or establishing gate operations. It should always be assumed that fragments are part of the charge as safe standoff distances are greater for fragments than for blast.

(3) If a bomber is identified, security personnel should train weapons on the bomber and maintain eye contact from behind cover. Ensure fields of fire have been identified and rehearsed to avoid fratricide and endanger innocent bystanders.

(4) Separate the subject from the IED: warn target that failure to comply will result in death. Give order to raise hands, take off outer garments and place on the ground. Have subject move a safe distance away from clothing and then handcuff. Close and negotiate tactics should not be attempted, as homicide bombers are trained to avoid surrender at all costs.

(5) Assume a fail safe cell phone or radio-controlled initiator could be used in the event that the bomber is incapacitated or hesitates. This tactic would normally involve a second suspect with a line-of-sight view of the bomber. Consider surveillance detection efforts to monitor the environment and deter enemy observers near the checkpoint or gate.

(6) If deadly force is employed, bullet impact may initiate the explosive charge(s). Therefore firing on the suspect should be undertaken from cover and not be aimed at mid-body.

(7) If the suspect is neutralized and there is no explosion, do not administer first aid. The explosive charge should be rendered safe by authorized EOD personnel only.

f. The following are TTP to consider to mitigate the VBIED threat at high risk vehicle checkpoints:

(1) Elements:

(a) A headquarters element to ensure command and control.

(b) A security element to provide early warning and observe flow of vehicles approaching the checkpoint.

(c) Traffic sentry to operate stop point forward of and controls traffic leading to checkpoint. Signs in the local language should be used to communicate instructions for negotiating barriers leading to search location.

(d) Search team to halt vehicles, conduct searches and direct cleared vehicles onward. One member should search the vehicle while the other team

members provide over watch.

(e) An assault element in fortified positions to overwatch checkpoint. This element should be prepared to engage (consistent with ROE) any vehicle that attempts to force its way through or poses a danger to the checkpoint.

(2) Checkpoints should present a robust security posture in order to discourage threats. Consider employing armored vehicles and crew served weapons in overwatch positions to support dismounted troops. Consider an antiarmor capability for security elements.

(a) A serpentine vehicle maze (barriers/freeway dividers) can be used to slow vehicles approaching the search area. A vehicle maze will enable security personnel more time to react to a vehicle attempting to run or attack the check point, as well as channel threat vehicles in escape lanes to a predetermined location for engagement.

(b) Hasty checkpoints should take advantage of terrain features/surrounding obstacles (bridges, highway/road intersections, reverse slope of a hill, just beyond a sharp curve) to slow vehicles as they approach the checkpoint. Deliberate checkpoints may require engineers or other support to emplace obstacles and barriers to channel traffic. Deliberate checkpoints should include holding/search areas with appropriate blast protection for personnel conducting searches.

(3) Suggested procedures:

(a) Instruct passengers to get out of the vehicle at a pre-designated and well-marked search area.

(b) All passengers should be instructed to come out with arms above their heads. Once out of the vehicle, instruct male passengers to lift their shirts in order to enable security forces to observe waist. If there is doubt, have them strip.

(c) Instruct one passenger to open all doors, hood, and trunk.

(d) Consider that women and children have also carried out attacks and ensure they are disarmed as well. Use female US military/host nation security personnel to search women and children in a separate, closed area.

(e) If any member or the checkpoint has any doubt about the vehicle, back everyone off and call for assistance.

(4) Suggested equipment – the following are mission enhancing tools at a high risk checkpoint:

(a) Loud speaker team with linguist. Time permitting, prepare

and emplace signs in the local language instructing drivers what to expect and do at the checkpoint.

(b) Explosive detector dog teams.

(c) Use of metal detector wands for physical searches, if possible, in addition to a crush and feel search.

(d) Stingers/caltrops (device that can be dragged across the road to puncture tires).

(e) Vehicle control and blast mitigation barriers.

(f) Separate search areas for small and large vehicles. Consider using trenches large enough for vehicles to enter so they may be searched. Vehicles can pull into the ditch and open all doors prior to search.

e. Man portable air defense system threat.

The purpose of this message is to emphasize to commanders and AT officers the importance of considering the man portable air defense system threat (MANPAD).

(1) The 28 November 2002 terrorist attack on an Israeli Airliner in Kenya highlights the potential manpad threat to US aviation interests, both conus and oconus. Commanders who own and/or are supported by air assets should consider risk and make decisions to alter, divert, or cancel air missions if the MANPAD threat is too great to mitigate. This is especially critical for locations transited by commercial air carriers moving our forces and equipment.

(2) Air mobility command (AMC) maintains a worldwide database with current intelligence and operations information that can assist. Commanders to reach prudent decisions pertaining to the MANPAD threat. The AMC intelligence combined risk assessment database offers both automated risk assessments known as the virtual threat assessor (VTA) program, and formal threat working group (TWG) virtual risk assessments known as the virtual threat assessor (VTA) program, and formal threat working group (TWG) virtual risk assessments. Both products offer such items as airfield information, terrorist, medical, military, information operations, and other threat information, along with archived briefings and open source information. The web address for these products is HTTP://WWW.AMCIN.SCOTT.AF.SMIL.MIL/VTA.

(3) Airfield security and local area assessments should be conducted to identify the area of vulnerability to the manpad threat (in terms of possible launch sites) to include the airfield arrival and departure corridors as well as potentially vulnerable ground targets such as parked aircraft or ground vehicle motor pools. A thorough assessment could include security forces, intelligence, counterintelligence, and operational personnel as well as local/host nation authorities.

(a) The defense intelligence agency-missile and space intelligence center has flight path threat analysis simulation (FPTAS) software that slows the local commander to quantify the areas of greatest MANPAD threat. FPTAS uses aircraft performance, flight path data, missile characteristics, and digital terrain elevation data to generate maps depicting area from which manpads could engage U.S. and allied aircraft. Commanders have used these maps to identify flight paths with minimum explosure to the MANPAD threat and have adjusted take-off/landing patterns to limit their explosure and utilize areas readily secured by ground troops. This software can be downloaded at the following web site:
HTTP://MSIC.DIA.SMIL.MIL/MS_HOME_PAGES/FPTAS/.

(b) Criteria to identify possible MANPAD launch sites include but are not limited to:

1. Cover and concealment – the ability of an object to provide protection for the terrorist from return fire and prevent detection by security force personnel.

2. Line of sight providing unobstructed view of the target.

3. Explosure time – the amount of time the intended target is vulnerable from an operational attack.

4. Distance to target and target recognition for the terrorist to positively identify the intended target.

5. Set up time required for a terrorist fire team to get into position to attack, and the time to discovery in terms of the amount of time it takes to detect a fire team once their weapons are exposed.

(4) There are two areas where commanders and antiterrorism officers should employ mitigation measures to counter the MANPAD threat: airfields/installation defense and reducing aircraft in-flight susceptibility.

(a) The following are points to consider in developing at plans in regards to airfield/installation defense and the MANPAD threat.

1. Once and analysis of possible launch sites is accomplished, prime manpad launch sites and vulnerable areas can be isolated by expanding the airfield area of control and reducing areas of vulnerability. The following mitigation measures may require coordination with local/host nation authorities:

a. Increased physical presence at prime launch sites. Visual observation of security teams is a strong deterrent.

b. focused and random patrols of vulnerable areas. Incorporate random patrols into the installation random antiterrorism measures program.

c. Implementation of technical equipment surveillance of vulnerable areas to include both launch and potential targets.

2. Ensuring personnel are educated on the MANPAD threat (to include component recognition), areas of vulnerability, and reaction plans. Develop and provide manpad awareness training for security force personnel and local/host nation law enforcement. Develop a MANPAD awareness program for neighborhood watch groups and local business/installation facilities in close proximity to airfields or along flight paths. The Defense Intelligence Agency Missile and Space Intelligence Center has a web site in their enduring freedom section that has a MANPADS link that is a good source for information on MANPAD systems (HTTP://MSIC.DIA.SMIL.MIL/MS_HOME_PAGES/SAM/SD_HOME_PAGES3.HTML).

3. Ensuring tight airfield access control procedures are in place for air field operations. Consider dispersal of parked aircraft to reduce damage from a MANPAD or rocket propelled grenade attack.

4. Developing and exercising contingency plans for responding to an incident of a manpad threat. Rapid reaction plans will facilitate the immediate capture of a terrorist team, even post attack, to deter/prevent future attacks and ease concern for air travel safety by the public at large.

(b) The following are points to consider in developing AT plans to reduce aircraft in flight susceptibility due to the MANPAD threat.

1. Establishing airfield specific procedures for the use of aircrew tactical countermeasures and/or tactics. Development and dissemination may require coordination with local/host nation authorities. Ensure aircrew awareness of possible effects of MANPAD on their aircraft. Ensure aircrews and flight operations are tied into the AMC intelligence combined risk assessment database to obtain current information on airfield security assessments.

2. Varying arrival and departure times of aircraft. Stagger the arrival times of normal scheduled missions to make arrival, departure, and ground times harder to predict for the terrorist.

3. Randomly changing approach and departure routes as a deterrent (in accordance with current federal aviation administration guidelines).

4. Limiting or discontinue use of landing lights within identified threat zones to reduce heat producing/targeting options.

5. In high threat areas or when intelligence has indicated a high alert status, coordinating and developing plans for engine-running offloads to minimize ground time.

Intentionally Blank

CHAPTER VII
TERRORIST INCIDENT RESPONSE AND TERRORISM CONSEQUENCE MANAGEMENT

"If historical experience teaches us anything about revolutionary guerrilla war, it is that military measures alone will not suffice."

Bgen S.B. Griffith, USMC
Introduction to Mao Tse-tung on Guerrilla Warfare, 1961

1. General

a. Terrorist Incident Response Management is a sequence of command, staff, and first responder actions to respond to a terrorist incident or other unique event and restore AT capability. The primary objective of Terrorist Incident Response Management is to limit the effects and number of casualties resulting from a terrorist attack. Commanders develop response measures to save lives, preserve health and safety, secure and eliminate the hazard, protect property, prevent further damage to the installation, and maintain public confidence in the installation's ability to respond to a terrorist incident.

b. Terrorism Consequence Management

~~b~~c. A commander's responsibility and authority to enforce security measures and to protect persons and property is paramount during any level of conflict. As such, it is incumbent upon the commander to plan for, and be capable of reacting to, a terrorist attack. ~~If the attack involves a chemical, biological, radiological, nuclear or high-yield explosive device, the number of casualties and the extent of the areas involved may quickly overwhelm organic resources.~~ Attacks employing CBRNE weapons may produce massive casualties or widespread destruction, which can quickly overwhelm organic resources. This situation is covered in more detail later in section paragraph 5.

~~c~~d. ~~This Chapter addresses management of a terrorist incident.~~ The focus of incident management is on the organic assets of an installation, ship, or base and the ability to cope with the situation using organic assets until outside assistance arrives. DODI 2000.16~~, *DoD Antiterrorism Standards*~~, requires all commanders to prepare installation-wide terrorist incident response measures and include them in the AT plan. The terrorist incident response measures should include procedures for determining the nature and scope of incidence response; procedures for coordinating security, fire, and medical first responders; and steps to reconstitute the installation's ability to perform AT measures.

~~d~~e. There are an unlimited number of potential terrorist incidents requiring a response. Developing separate courses of action for each is an unrealistic task. To prepare for the most probable, or likely threats, AT Plans should address (at an absolute minimum) each potential threat identified through the Threat Assessment Process.

Additionally, broad category threat response plans should be developed in order to provide an initial response to threats not yet identified through the Threat Assessment Process.

2. Terrorist Incident Management Planning

a. The establishment of a mechanism to respond to a terrorist incident is an essential element of the ~~DOD CbT Program~~ DOD AT program. Normally, the installation, base, or unit commander identifies an office or section, or designates personnel from various sections, who act as the principal planning agency for special threats and who comprise the Emergency Operations Center (EOC) (see paragraph 3.d.) during an actual crisis. One effective method for determining what areas should comprise the planning and execution of the response is to use the WMD response functions.

b. There is no requirement to have a separate terrorist incident management plan. However, DODI 2000.16 requires that the AT Plan address terrorist incident response measures.

3. Initial Response

a. Onset of a Terrorist Incident: The onset of a terrorist incident begins with the detection of an unlawful act of violence or threatened violence. Detection may result from routine surveillance performed by an installation or facility intrusion detection system, guard or security force, an unusual incidence of an infectious disease in the case of bioterrorism, or ~~aware~~ vigilant DOD-affiliated or community persons. Once detection of a criminal act occurs, first responding security or law enforcement personnel must perform an initial assessment.

b. Initial Response Force

(1) ~~On-duty Security Forces/Military Police patrols or guard personnel usually provide initial response to a terrorist attack. The initial response force is usually under the control of the on-scene senior officer or noncommissioned officer assuming responsibility.~~ The initial Response Force consists of the forces identified in the installation's/ship's terrorist response plans with on-scene command relationships and chain of command clearly established in the same sources. At facilities controlled by the Defense Agencies, the initial response force may be under the control of a senior civilian security or DOD law enforcement official. Once the initial response force has responded to the incident and determined the circumstances, the installation commander should activate required forces and begin notification procedures for military and civilian authorities.

(2) The initial response force should immediately identify and report the nature of the situation, isolate the incident, and contain the situation until relieved by the reaction force commander. Initial response force actions are critical. ~~Each~~ Every

shift ~~of the daily security force~~ must have trained personnel who are aware of the threat and are capable of reacting promptly to any new development.

(3) For example, if the attack is a bombing, ambush, assassination, or firebombing, the terrorists may escape before additional forces arrive. In these cases, the initial response force should provide medical aid, seal off the crime scene, and secure other potential targets in case the initial attack was a diversionary tactic. If the event is a hostage/barricade situation, the initial response force should seal off and isolate the incident scene to ensure no one enters or leaves the area. The initial response force must also be prepared to locate witnesses and direct them to a safe location for debriefing. ~~For foreign incidents, t~~The initial response force must also be prepared to interface with local law enforcement or emergency service personnel, host nation police, or military forces ~~that may also be~~ responding to the incident~~.~~ in accordance with existing Host Nation Support Memorandums of Agreement and/or Status of Forces Agreements:

c. Installation/Base Commander. The installation/base commander, depending upon established standing operating procedures (SOPs) should activate the installation's EOC. Additionally, the commander should notify specialized response forces, and immediately report the incident to the appropriate superior military command EOC, military investigative agency, FBI, civilian authorities, and if a foreign incident, to host nation authorities and the US Embassy, as required.

d. Emergency Operations Center

(1) The EOC serves as the command post ~~at a predetermined~~ location. Communications are established immediately with the initial response force containing the situation, the specially trained operational response force preparing to take over or augment the initial response force, and other critical participants ~~as pre-designated~~ in the EOC's SOPs. There are usually three standard secure communications circuits: command net (administrative matters, support, routine traffic), tactical net (operations), and intelligence net. If necessary, a dedicated net for negotiations may be necessary if a landline cannot be established with the terrorist.

(2) The EOC should distribute responsibilities into four basic functions:

(a) Operations. Responsible for first responders (fire, security, and medical); hazardous materials; bioenvironmental engineering; safety; and public affairs.

(b) Logistics. Responsible for service (communications, power, food) and support (shelters, supplies, etc.).

(c) Planning. Responsible for amending and developing plans to address the changing circumstances.

(d) Administration. Responsible for tracking personnel casualties or fatalities, notifications, report, and contracting services as necessary.

e. Confirmation

(1) Since jurisdiction depends on whether the incident is terrorist related, it is important for the response force to identify the type of incident as quickly as possible. If the FBI or host nation assumes control, then the response force must be prepared to coordinate the operational handover and assist as needed.

(2) The initial or specialized response forces may be required to provide outer perimeter security as well as be prepared to manage the entire event. They must also be prepared to turn over responsibility for resolving the incident to ~~host government~~ HN security forces if overseas or the FBI if within the United States and in the event the FBI seeks to exercise jurisdiction over the containment and resolution phases of the incident. These installation/base forces must always prepare for the most resource-demanding contingency. This level of readiness requires considerable sustainment training.

f. DOD installation military commanders and civilian managers have responsibility and authority for initial response, containment, and resolution of criminal incidents that occur on DOD facilities under their control prior to relinquishing that authority to the appropriate jurisdictional lead agency. In all cases, however, command of military elements remains within military channels. For detailed discussion on jurisdiction, authority, responsibilities, and other legal considerations concerning response to criminal incidents, see Chapter IV and Appendix J.

4. Follow-on Response

The response to a terrorist incident varies depending on the nature and location of the incident. Generally there are three distinct phases through which an incident may evolve although many incidents do not develop beyond the first phase.

a. Phase I: Locally Available Resources. Phase I is the commitment of locally available resources, including available Security Forces/Military Police patrols or guards and available backup units. Civilian contract guard services should not be used as part of an initial response force for a terrorist incident unless there is no Federal law enforcement or Security Forces/Military Police available. Civilian contract guard services should generally be restricted to perimeter security duties, traffic control, and crowd control activities. All initial responders, such as fire as fire and medical personnel must understand and be trained to protect the incident location as a crime scene within established protocols. Ideally, all law enforcement or security personnel are familiar with local SOPs for terrorist incidents and have practiced these procedures as part of their unit-training program. They must be prepared to secure, contain, and gather information at the scene until the beginning of Phase II. While securing and containing the incident scene, response forces must be alert to the fact terrorist incidents often include

diversionary tactics and secondary attacks with the desired purpose of harming first responder personnel. The evacuation of threatened areas is a high priority function.

b. Phase II: Augmentation of Initial Response Force. Phase II is the augmentation of the initial response force by additional law enforcement/security personnel and/or a specially trained response force, such as Special Reaction Team (SRT)/Emergency Service Team (EST), FBI hostage rescue teams, or host nation tactical units. On many installations, the initial response force and the augmentation force are essentially the same. This phase begins when the EOC is activated. During this phase, either the FBI or the host nation may assume control jurisdiction over the incident. If that occurs, installation forces must be ready to support the operation. The installation specially trained response force must be ready for employment in this phase of the operation. In any country that a terrorist incident against an American facility/unit occurs, the DOS and the US Embassy shall play the key role in coordinating the US Government and host country response to such an incident.

c. Phase III: Commitment of Counter-Terrorist Resources. Phase III is the commitment of a specialized team from the FBI, the Department of Defense, or host nation counter-terrorist force. In this phase, steps are taken to terminate the incident. Incident termination may be the result of successful negotiations, assault, or other actions, including the surrender of the terrorists. Because identifying the terrorists, as opposed to the hostages, may be difficult, it is important that the capturing forces handle and secure all initial captives as possible terrorists.

Joint forces must be prepared to play an active security role throughout all three terrorist incident phases.

5. Initial Response to a CBRNE Attack

a. Installations have the requirement for an immediate response capability to ensure critical mission continuity and save lives during a CBRNE incident and to

mitigate the situation (DOD Instruction 2000.18, *Department of Defense Installation Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive Emergency Response Guidelines*). National-level responders may not be immediately accessible ~~n~~or available to respond to an installation's needs. Therefore, each installation must plan for the worst-case scenario by tailoring its response for each functional area, based on its organic resources and available local support through MOAs/MOUs. The situation may dictate that the installation not only conducts the initial response, but also sustains response operations.

b. In the event of a terrorist CBRNE incident, the commander should direct the following complementary sets of actions:

(1) Activate mass notification telling personnel to shelter in place, evacuate or take other appropriate action.

(~~1~~2) Activate the installation's initial response elements and local MOAs / MOUs.

(~~2~~3) Initiate the DOD notification process; and

(~~3~~4) Request resources to augment the installation's response capabilities.

c. Installation commanders are responsible for ensuring their first responders have a plan and are equipped, trained, and exercised on the plan for responding to an incident involving CBRNE.

d. Installations are required to have incident management plans. One effective way to develop these plans is by the use of weapons of mass destruction response functions (WMDRFs). The WMDRFs parallel the national-level FEMA Emergency Support Functions (ESFs) to the greatest degree possible. This parallelism ~~shall ensure~~ ensures that if there is a need for Federal assistance, incoming support can easily transition into the appropriate functional areas on the installation. The Installation Antiterrorism Program and Planning Tool (IPPT) uses the WMDRFs to systematically address each of the installation response functional areas. From these Response Measures, the installation planners should create installation specific action sets or implementation instructions. These action sets should include who, what, when, where, and how the lead staff element shall carry out the response measure. Once planners have carefully prepared discrete actions sets, it is recommended they be placed in a response matrix.

e. Terrorist CBRNE incidents, or threats of terrorist CBRNE acts, may overwhelm an installation's minimum capability to adequately detect, assess, or contain the threat. The Department of Defense, like most other local, State, or Federal entities, has neither the authority nor the expertise to respond unilaterally to all aspects of terrorist CBRNE threats or acts. ~~The tenets of the National Response Plan shall help an~~

~~installation develop its response based on crisis and consequence management.~~

6. Special Considerations (see figure VII-1)

a. Establishing Communications. A crucial aspect of implementing the AT plan is establishing secure communications among the forces in the incident area and the EOC. Once this is done, all other elements of the communications plan are activated. Communications personnel must be able to respond to changing needs during the incident and be able to maintain, over a prolonged period, the communications channels included in the AT plan.

b. Evidence. Although the primary goal is ending a terrorist incident without injury, another goal is the successful prosecution of terrorists. Witness testimony, photographic evidence, etc., are important in achieving a successful prosecution. Maintaining the continuous chain of custody on evidence obtained during an incident requires documenting the location, control, and possession of the evidence from the time custody is established until presenting the evidence in court. Failure to maintain the chain can result in exclusion of the evidence. Types of evidence for which the chain must be established include, but are not limited to:

(1) Photographs taken during the incident.

(2) Physical evidence, including any item(s) used by the terrorists.

(3) Tape recordings of conversations between terrorists and hostage negotiators.

(4) Demand notes or other messages recorded by written, audio, or video means prepared by the terrorists.

(5) Sample collection, including samples collected at the scene taken during initial and follow-on response.

c. Disposition of Apprehended Personnel. Apprehended military personnel must be handled according to Service regulations and applicable installation SOPs. In the ~~U.S.~~US, civilian detainees must be released to the FBI or US Federal Marshals for disposition. In foreign incidents, civilian detainees may be processed according to the SOFA, diplomatic note (DIPNOTE), or other agreements with that particular country. The Staff Judge Advocate should be consulted prior to releasing any individual to Host Nation authorities. In coordination with the Staff Judge Advocate (SJA), an after-action report should be prepared within ~~7~~ seven working days after termination of the event.

d. Reports. Reporting to higher headquarters is an important element in any special threat or terrorist situation. Each Service and command has a reporting procedure that requires a timely report of the incident to higher military authorities. The crisis management plan should dictate required reports and timelines for notification. An after-

action report should be prepared within seven working days after termination of the event. This should include all staff journals and other documentation to include detailed information concerning disposition of evidence and captured individuals. The SJA and law enforcement personnel should ensure this report is in sufficient detail to meet prosecution requirements.

e. Public Affairs (PA). Principal PA objectives of a terrorist incident crisis management plan are to ensure accurate information is provided to the public (including news media) and to communicate a calm, measured and reasonable reaction to the ongoing event.

(1) PA programs should attempt to:

(a) Identify terrorist activities, as criminal acts not worthy of public support.

(b) Reiterate US policy on terrorism that identifies all terrorist acts as criminal acts, mandates no concessions to terrorists, refuses to pay ransom, and isolates those nations identified as encouraging, supporting or directing terrorism; and

(c) Support DOD PA strategy on releasing information pertaining to antiterrorism plans, operations, or forces involved in antiterrorist operations.

(2) The DOJ has lead PA responsibility for incidents occurring on US territory if the FBI assumes jurisdiction for resolving the incident. The Office of the Assistant Secretary of Defense (Public Affairs) (OASD (PA)) supports the DOJ in providing specific PA support.

(3) When US military forces ~~security or combating terrorism forces~~ are employed, the ~~Department of Defense~~DOD provides a spokesman for addressing ~~dealing only with security or combating terrorism forces~~ military operational matters.

(4) The DOS coordinates PA during terrorist incidents overseas. The DOS may delegate the PA responsibility to a designated DOD representative.

(5) The OASD (PA) is the single point of contact for all PA aspects of US military CbT actions. While there is no mandatory requirement to release information, installation commanders are advised to exercise prudent judgment on such matters and coordinate actions through PA channels to OASD (PA).

(6) When the EOC is activated, it should include the activities of the public affairs officer (PAO) and media center. The media center should be located in a separate location away from the EOC. The PAO shall prepare media releases and conduct briefings at the media center during the incident. The PAO shall use information obtained from EOC activities. PA shall coordinate with EOC personnel, and clear all information with the commander, prior to release. The PAO must be fully

knowledgeable of the situation as it develops. The media representatives should not have direct access to hostages, hostage takers, communications nets, or anyone directly involved in a terrorist incident unless the PAO has cleared such contact with the EOC. DOD experience with media representatives has shown that bringing them in early under reasonable conditions and restrictions commensurate with the risk and gravity of the event, and providing them thorough briefings, maintains DOD credibility and preserves freedom of information.

f. Immediate Post-Incident Actions. During the immediate post-incident phase, medical and psychological attention, along with other support services, should be given to all personnel involved in the operation, including captured terrorists. A final briefing should be given to media personnel; however, they should not be permitted to visit the incident site until the investigation is complete and such access is cleared by appropriate officials. Because of the criminal nature of the terrorist event, the site must be secured until the crime scene investigation is completed by the appropriate investigative agency. It is also imperative to record every action that occurred during the incident.

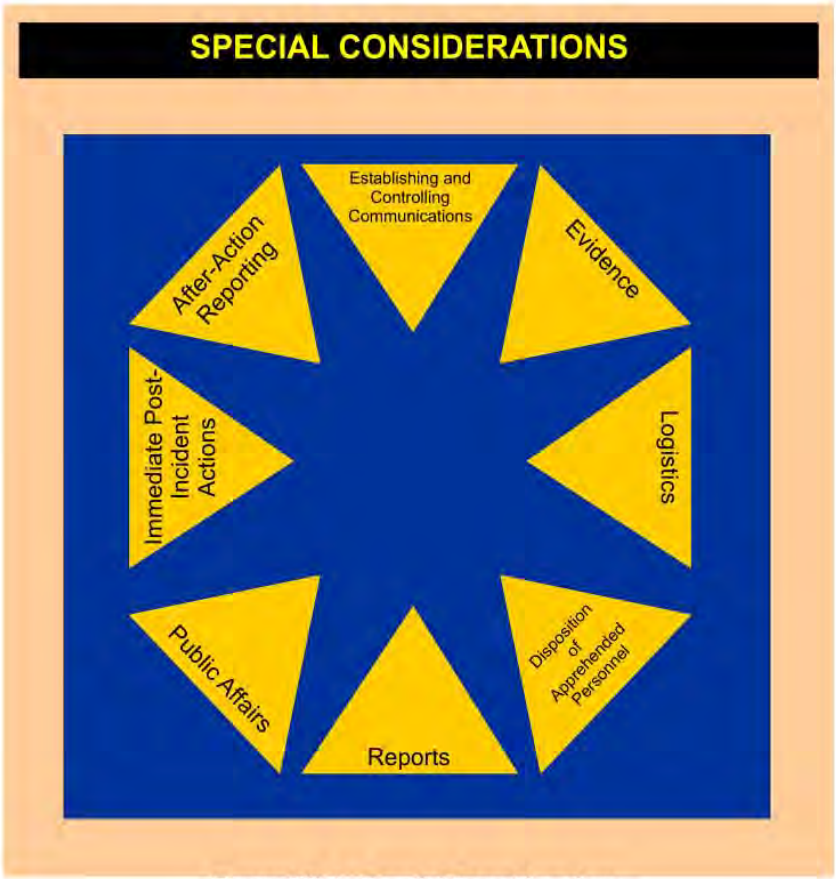

Figure VII-1. Special Considerations

Intentionally Blank

APPENDIX A
THREAT ASSESSMENT

1. Introduction and Overview

The AT Risk Management process begins with an assessment of the terrorist threat to DOD personnel and facilities. The AT Threat Assessment is used to identify the terrorist threats posed to DOD assets and/or the threats that could be encountered in executing a mission.

2. Terrorist Threat Assessment

a. The threat assessment system is vital to developing and disseminating terrorism warnings. Specific warning information - time, date, place, those involved, and method of attack - is rarely voluntarily provided by terrorists. Careful threat analysis is required to detect and correctly evaluate pre-incident indicators of a terrorist attack, so timely warning messages can be issued.

b. Threat analysis provides the intelligence officer with information upon which to base warnings.

c. Threat information for AT programs is diverse and includes foreign intelligence, open source materials, domestic criminal information, and information from federal, state, and local governments.

(1) Open source and publicly available information may be collected, retained, and disseminated as prescribed in Executive Order 12333, *United States Intelligence Activities*, DOD 5240.1-R, *Procedures Governing the Activities of DoOD Intelligence Components That Affect United States Persons*, and DOD Directive 5200.27, *Acquisition Of Information Concerning Persons And Organizations Not Affiliated With The Department Of Defense*. Organizations engaging in these activities must ensure they are properly authorized to do so. Examples of open source material include:

(a) News media (print and broadcast) may provide good information on terrorism. News organizations often are the first to report many major terrorist incidents and include in-depth reports on terrorist individuals or groups. Such reports can provide analysts with insights into terrorist group goals and objectives, the motivation of individual members of terrorist organizations, modes of recruitment, training and training methods, and tactics of attack. Terrorist groups frequently use the media to promote their cause.

(b) Scholarly publications.

(c) Unclassified US and foreign government publications.

(d) Press releases.

(e) Political tracts, handbills, posters, flyers, and leaflets often distributed by organizations committing, supporting, or opposing terrorist actions may reveal their objectives, tactics, and possible targets. Such information is often placed into the public domain as part of a campaign of terror.

(f) The World Wide Web (Internet) provides terrorists an outlet to spread propaganda, recruit new members, and aid in fundraising. In addition, the web provides a wealth of information to include: training and training methods, weapons, and weapons usage. Only specially trained counterintelligence personnel should access these sites. Terrorist organizations have shown increased sophistication in the area of information warfare and casual visits to their sites may inadvertently provide them intelligence information on who may be interested in their activities and/or expose the untrained visitor to a computer hacker attack.

(2) Commercial data services may offer timely information about international or military affairs that often include information regarding terrorist incidents. Such data services often rely on foreign news media. Some data services maintain their own network of sources. Information services are provided on a subscription or fee-for-service basis.

(3) The Defense Criminal Investigative Organizations (DCIOs) and military and civil law enforcement agencies collect criminal information. Since terrorist acts are criminal acts, criminal information is a lucrative source for terrorist intelligence. Local military criminal investigative offices maintain current information in accordance with DOD regulations governing retention of criminal information. Such material may assist managers and military commanders in the assessment of the local terrorist threat.

(4) Government information refers to materials collected, analyzed, and disseminated under official auspices. It includes, but is not limited to, scientific and technical reports, political and economic reports, crime and terrorism statistics, policy statements, legislation, and official correspondence.

(a) Some government information may be open source, available to all persons who either request or purchase it.

(b) Government information may also be restricted or have limited distribution only within government agencies. Such information might include post-conviction court records, export/import license applications, immigration records, or financial securities registration information not released to the public.

(c) Government information also includes data and analyses derived from intelligence classified sources. Exchanges with local government agencies through, for example, "cooperative arrangements" can also augment regional information.

(5) Local information can come from individual service members, civil servants, family members, and individuals with regional knowledge, such as college faculty or cultural organizations. Local crime or neighborhood watch programs can also be valuable sources of information and can serve as a means to keep individuals informed in dispersed and remote areas.

(a) Local information is often of critical importance as it is collected and passed through either law enforcement and/or intelligence channels to the national intelligence organizations. It is frequently invaluable to analysts confirming news media or other open source accounts of terrorist activities. It can provide early warning of potential terrorist activities, allowing law enforcement and combating terrorism measures to be initiated in a timely manner to thwart or minimize the effects of a terrorist attack.

(b) A critical element of local information is obtained from individual service members, their families, and civilian employees at DOD facilities who report any suspicious activity they observe. It is critical that all these personnel receive frequent, thorough training regarding the recognition and reporting of suspicious activity. Such reports, even those that may appear frivolous, must receive immediate investigation by law enforcement and counterintelligence personnel.

d. Access to Intelligence

(1) Terrorist threat information flows back and forth in the field, and among the combatant commanders, the Services, and the DIA. At each level, it is integrated, fused, and assessed in accordance with regulations and DOD Directives governing the security and dissemination of intelligence and law enforcement information. Terrorist threat information and analytical products are also disseminated from the national, DOD, Service, Agency, and combatant commander levels to all echelons of command and individual Defense Agency activities as appropriate.

(2) The combatant commanders, through their Intelligence Directorates and Counterintelligence Staff Officer, and in consultation with the DIA, embassies' staffs, country team, and applicable host nation authorities, assess intelligence specific to their areas of ~~operation~~ responsibility and issue intelligence reports, advisories, and counter intelligence reports to the units within the combatant commander's control or AOR. This intelligence dissemination network is the backbone for communicating intelligence information throughout the region and to the national level.

3. Terrorism Threat Level Assessment Methodology

a. This DOD methodology assesses the terrorist threat to DOD personnel, facilities, and interests. The methodology is used by all DOD Components to determine the level of terrorist activity in a specific country, region, or locale. This methodology does not address threats from conventional forms (i.e., hostile conventional armed forces) and/or the criminal threat (if unrelated to known or suspected terrorist activity).

(1) Threat levels are assigned based on available intelligence and an analytical assessment.

(2) Threat levels describe an environment, not a probability of attack.

(3) Terrorist threat levels do not allocate protective resources.

(4) Issuance of a Terrorist Threat Level judgment is not, in and of itself, a formal warning vehicle.

b. Threat analysis is the process of compiling and examining all available information to develop intelligence indicators of possible terrorist activities.

c. The Department of Defense has identified several factors to identify the collection and analysis of information from all sources concerning terrorist threat(s). These factors are used in making terrorist threat analyses on a country-by-country basis.

d. Methodology Factors

(1) Operational Capability is the acquired, assessed, or demonstrated level of operational capability to conduct terrorist attacks.

(a) Group Tactics focuses on the attack methods used by the group. What type of attack has the group conducted in the past? Has the group conducted large or small-scale bombings, kidnappings, assassinations, drive-by shootings, or other assaults? Has there been any indication the group has any new capabilities? Has the group been notably unsuccessful in any types of attacks?

(b) Mass Casualty Capability/Willingness. Does the group have the capability and willingness to conduct mass casualty attacks? Has the group conducted such attacks in the past? Has the group shown an interest in CBRNE material?

(c) Targeting. Does the group conduct attacks intended to maximize casualties, i.e., conducting an attack at peak business times, or placing secondary improvised explosive devices to target first responders? Does the group attempt to limit damage to property only, by placing IEDs after business hours or in remote locations?

(d) State Sponsorship. Does the group have state sponsorship? Who is the state sponsor? What type of intelligence/logistics/training/funding is provided? Is support from one or more Governments? If so, which ones?

(e) Group's Operating Area. Is the group indigenous, regional, or transnational? Can indigenous groups operate regionally or transnationally?

(f) High Technology Access. Does the group have access to high technology? Does the group use computers? If yes, to what extent? Can the group conduct sophisticated technical surveillance or employ advanced IEDs? What type of equipment is used? Where did the group get the equipment? Who trained the group?

(g) Method of Operation. What is the group's method of operation? A group shall likely continue to use techniques and tactics that have been successful in the past.

(h) Professionalism. What is the group's overall professionalism? Has the group consistently carried out successful sophisticated attacks? Has the group demonstrated a high or low degree of tradecraft?

(i) Different Tactics Equate to Different Threats. Different tactics result in different degrees of threat. A group that conducts property attacks presents less of a threat than one that has conducted assassinations or attacks with large vehicle borne IEDs.

(2) Intentions are the stated and/or the actual history of attacking US interests.

(a) Recent Attacks. Has the group conducted a recent terrorist attack? Type of attack? Weapons type? Were any pre-incident indicators noted? Was outside support used? Did the group claim the attack?

(b) Anti-US Ideology. Does the group have an anti-US ideology? Is the ideology stated publicly? What is the group's main opposing points with the US? What trigger events could entice the group to act?

(c) Anti-Host Nation Ideology. Does the group have an anti-host nation ideology? Does the group consider US aid/support a hindrance to its goals? At what point would the group consider attacking US interests due to this support?

(d) Attacks in Other Countries. Has the group conducted terrorist attacks in other countries? Where? What type of attack? What type of support network was in place?

(e) Response to Current International Events. Has the group ever responded to an international event with a terrorist attack? What was the event? What type of response? Has the group ever publicly denounced an international event involving the US? Did they threaten US interests?

(3) Activity. A terrorist group's activity in a country may not always be related to operational planning or present a threat to US/host nation interests. Many groups use countries as support bases and may not want to jeopardize their status by conducting a terrorist act there. Analysts must determine the group's activity by

examining influencing elements and keeping in mind that the situation is always fluid and subject to change. Some of the key elements in evaluating activity are:

(a) Presence. Is a group present but inactive?

(b) Fund-raising and Safe Haven. Does the group use the country for fund raising? What type of fund raising? How much money is generated? What is its intended use? Is any of the money funneled to other locations or groups? Does the group use a country as a safe haven?

(c) Suspected Surveillance, Threats, and Suspicious Incidents. Has the group been known to conduct surveillance? Is the group proficient at surveillance? What does the group do with the surveillance information? Has the group threatened DOD/US interests? How does the group conduct surveillance? Have there been any suspicious events that could be linked to the group?

(d) Changes in Philosophy Impacting Targeting. Has the group shown any signs of changing philosophies? Does the philosophical change include targets? Is the Department of Defense affected?

(e) Level of Involvement with External Cells. How does the local leadership interact with external leadership? How much contact is normal? Does the group have connections with other cells? Do the cells train together? Do they share intelligence?

(f) Key Operative Movement. Has there been any noted movement of key operatives? If so, from where to where? Was the movement covert? Was there any reaction from other cells? What was the purpose of movement? Were code words used?

(g) Contingency Planning. Has any planning been noted? Who/what are the targets? How were past plans executed? Who conducted the planning? Was outside help used/requested? Did any attacks occur after planning was noted? How much time elapsed?

(h) Disruptions by US or Host Nation Security Elements. Have US or host nation security forces disrupted any of the group's activities? If host nation only, does the group perceive US involvement? What caused the disruption? What was uncovered by security? How does it affect the group's operational capability in country?

(i) Identification of Weapons Caches. Have weapons caches been uncovered? What types of weapons? Are the weapons consistent with the group's past weapons usage? Who supplied the weapons?

(j) Cell Activity (Operational or Support). What type of activity does the group mainly conduct in country? Operational? Support? Size of cells? Number of cells?

(k) Credible Indications of Targeting US Assets. Is there any indication the group is targeting US assets? At what stage of the targeting process was the plan uncovered? Timing? Specific target? Location?

(l) Assessment of Intelligence Reporting Regarding Terrorist Activity. What type of intelligence is being reported (Signal Intelligence [SIGINT], HUMINT, etc.)? Source of reporting? Reliability? Access?

(4) Operating Environment. How the overall environment, to include political and security considerations, influences a terrorist group's ability and motivation to conduct an attack. Influencing factors include:

(a) DOD Presence. What is the DOD presence in the country? Size? Location? Duration of stay? What are DOD personnel doing in country (training, support, security, etc.)? What is the terrorist perception of DOD significance? How politically sensitive is the DOD presence? What could entice the terrorists to attack DOD interests?

(b) External Influencing Factors. Is the host country at war? Could this influence a terrorist group to attack? Is there active insurrection? Is the terrorist group involved in the insurrection?

(c) Host Nation Security and Level of Cooperation. Can host nation security (to include national law enforcement, paramilitary and military institutions) maintain social order? How well are security forces trained to respond to terrorist incidents? Type of equipment available for security forces? How are forces dispersed around the country? Does host nation cooperate with US authorities? Does host nation share information?

(d) Political Influences Affecting Motivation to Attack. What political influences are affecting the group's motivation to attack? Has host nation cracked down after previous terrorist acts?

4. Terrorist Threat Level

a. The Department of Defense uses four threat levels to define the degree to which the environment is conducive to conducting terrorist operations in a specific country, region or locale by using the factors and elements described above. The four threat levels are Negligible, Low, Medium, High, and Critical.

(1) High. Anti-US terrorists are operationally active and use large casualty producing attacks as their preferred method of operation. There is a substantial DOD presence and the operating environment favors the terrorist.

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

(3) Moderate. Terrorists are present but there are no indications of anti-US activity. The operating environment favors the Host Nation/US

(4) Low. No group is detected or the group activity is non-threatening.

b. A Terrorism Warning is issued when credible specific targeting information is obtained and is formally linked to the methodology (see paragraph 7).

c. Warning Report. A report issued by the DIA when a terrorist group is operationally active and US interests are specifically targeted. A warning report may be issued at any threat level (see paragraph 7).

5. Changes in Terrorist Threat Level Declarations

a. Analysis of terrorism is an ongoing process. Although each analysis relies on information included in previous assessments, judgments with respect to threats to DOD-affiliated personnel, facilities, and assets begin anew with each analysis. No formal escalation ladder of terrorist threat level exists. Terrorist threat level designations for each country are applied on the basis of current information analysis.

b. The DIA sets the DOD Terrorism Threat Level in a particular country. The geographic combatant commanders can also set terrorism threat levels for specific personnel, family members, units, and installations within their AOR, using the definitions established by the DIA. Terrorist threat level designations can change without passing through any intermediate steps. A new terrorist group could initiate a series of attacks on DOD personnel or facilities, which could cause a threat level to rise several levels or initiate a Warning Report.

c. Terrorism threat levels should not be confused with FPCONs. An FPCON is a security posture promulgated by the commander in consideration of a variety of factors (e.g., a terrorism threat assessment, terrorism threat levels, etc.). Terrorism threat levels should also not be confused with the Threat Conditions associated with the National Homeland Security Advisory System.

6. Threat Warnings

a. Terrorist threat warnings for the Department of Defense use two mechanisms: Community Alerts/Advisories/Assessments and Defense Terrorism Warning Reports. The Intelligence community system issues coordinated Terrorist Threat Alerts, Advisories, and Assessments. The DIA is a member of the national intelligence community along with the FBI, the CIA, the NSA, the Department of Energy, the Department of Treasury, the Department of Homeland Security, and the Department of State. The Interagency Intelligence Committee on Counterterrorism is authorized to provide national-level terrorism warnings to US government organizations and customers. The Department of Homeland Security is responsible for disseminating terrorist threat warnings for attacks in the homeland. DIA is charged with assessing and disseminating terrorism threat warnings concerning DOD personnel and facilities, both domestically and overseas, to DOD personnel.

b. The DOD Defense Indications and Warning System (DIWS) comprises a second, independent system in which DOD members at any level may initiate unilateral threat warnings. These are termed Defense Terrorism Warning Reports. Warnings within the DOD system generally stay within the system and are primarily for use by the DOD Components. DOD Terrorism Warning Reports are active for a maximum 30-day period with one 30-day extension authorized.

c. Basic Warning Report Procedures within the Department of Defense

(1) DIWS Terrorist Threat Warning Reports may be prepared and issued by any member of the DIWS system. DIA is required to propose a National Intelligence Community Alert or Advisory prior to issuing a unilateral DIWS Terrorism Warning Report.

(2) Individual DOD components also have the right to independently notify their members of impending threats. If a DOD component intelligence activity receives information that leads to an assessment of an imminent terrorist attack, it may exercise its right to issue a unilateral warning to its units, installations, or personnel identified as targets for the attack. If the DOD component intelligence activity issues a unilateral warning, it must label threat information disseminated as a unilateral judgment, and must inform DIA of its action.

(3) Warnings are issued when specificity of targeting and timing exist or when analysts have determined that sufficient information indicates that US personnel, facilities, or interests, particularly those of the Department of Defense, are being targeted for attack. Warnings need not be country-specific. A warning may cover an entire region or the world. The key to a warning is recognition that the pre-incident indicators for an attack are present.

(4) DIWS Terrorism Warning Reports are specific products. When issued, they perform a number of functions. They are unambiguous - it is clear to the recipients they are being warned. Warnings are intended for distribution up, down, and laterally through the chain of command - not just downward. Warnings of impending

terrorist activity are likely to have national implications and shall be provided routinely to decision-makers at the policy level of the US Government.

d. No "Double Standard". Following the terrorist bombing of Pan Am flight 103 over Lockerbie, Scotland, on December 21, 1988, the US Government adopted a policy of "No Double Standard" (see Public Law 101-604, *Aviation Security Improvement Act of 1990*). No terrorist threat warning shall be issued solely to US Government consumers IF the general public is included in, or can be construed to be part of, terrorist targeting. Terrorist threat warnings may be issued exclusively within government channels only when the threat is only to government targets. The DOS, overseas, is the sole approving authority for releasing terrorist threat information to the public

7. Installation Level AT Threat Assessment Requirements and Activities

a. Commanders down to the installation or tenant level task the appropriate organizations under their command to gather, analyze, and disseminate terrorism threat information. When organic intelligence/counterintelligence/law enforcement assets are not available, commanders should request support from higher authority. The full range of intelligence, counterintelligence, and law enforcement capabilities shall be utilized in support of distinct and separate threat assessment requirements: annual threat assessments and ongoing assessment of the local threat.

b. Annual Threat Assessment. Installation commanders shall, at least annually, prepare a terrorism threat assessment for those personnel and assets for which they have AT responsibilities. Whereas DOD Threat Methodology focuses on the degree of activity of known terrorist groups, the annual threat assessment seeks to identify the full range of feasible terrorist capabilities (weapons, tactics, techniques, and methods of attack) that could reasonably be used against the installation or its personnel. Even in the absence of a current known threat group, an assessment is a necessary input to the required annual VA and for planning physical and procedural countermeasures. Annual threat assessments should include all likely or feasible WMD including CBRNE threats.

c. Threat Matrix. Preparation of the annual threat assessment requires careful analysis of known local threats, together with estimates of relevant national and transnational threat capabilities. Locally derived, open-source information regarding the availability of weapons and component materials in the area is also necessary in developing the range of threats. Threat analysts preparing the assessment should differentiate threats likely to be used inside the perimeter from those more likely to be used outside the perimeter to aid in the VA and development of countermeasures. The threat matrix unambiguously establishes the range of specific threat capabilities that shall be used to analyze vulnerabilities and plan countermeasures. The threat matrix is a planning tool which ensures that security and procedural countermeasures are economically designed to counter specific threats or mitigate specific vulnerabilities, and that the risk remaining is well understood by commanders making risk acceptance decisions.

d. Both installation and unit commanders shall assess the terrorist threat for probability and severity of occurrence. Probability is the estimate of the likelihood that a threat shall cause an impact on the mission or a hazard to the installation. Severity is an estimate of the threat in terms of the degree of injury, property damage, or other mission-impairing factors. By combining estimates of severity and probability, an assessment of risk can be made for each threat. A matrix may be used to assist in identifying the level of risk. The outcome of this process is a prioritized list of threats. The highest priority threat is the one that poses the most serious risk in terms of likelihood and severity. This list of prioritized threats shall be used to evaluate the acceptability of certain risks and which risks for which to make decisions concerning the employment of resources and other actions that reduce vulnerability. This assessment should be recorded as a record/baseline and updated regularly as the threat changes. If installation and unit commanders do not have the resources to assess the threat for probability and severity of occurrence, they should coordinate with their next higher echelon to assist with this requirement.

e. Unit commanders should also conduct a variation of the AT Annual Assessment, but apply it to the conduct of their unit mission. Threats should be listed that affect the unit as it conducts its mission. The output of this assessment is a list of terrorist threat capabilities associated with each phase of the operation.

f. In addition to preparing an annual threat assessment, commanders must also continuously assess local threat information so appropriate FPCONs can be set. Commanders at all levels shall forward up and down the chain of command all information pertaining to suspected terrorist threats, or acts of terrorism involving DOD personnel or assets for which they have AT responsibility. Threat information shall be used in the determination to raise or lower the present Force Protection Condition. Continuous threat analysis also supports the warning of suspected target facilities or personnel through the installation's mass notification system when the information relates threats of an immediate nature.

Intentionally Blank

APPENDIX B
VULNERABILITY ASSESSMENT

1. General

A VA is the process the commander uses to determine the susceptibility of assets to attack from threats identified by the AT threat assessment. The VA answers the question "what kind of attack is the asset most/least vulnerable to?" DODD 2000.16, *DoDD Antiterrorism Standards*, provides authoritative standards regarding both installation and deploying unit Vulnerability Assessments. Vulnerabilities exist at every installation as a result of the terrorist threat faced. Vulnerabilities are always there, no matter the policies, procedures, structures and protective equipment. Although terrorist threats cannot be controlled, they can be assessed and the vulnerability of assets to those threats can be mitigated. Identifying and understanding vulnerabilities is important in determining how well an asset shall be protected from loss. Vulnerabilities are also the component of overall risk over which the commander has the most control and greatest influence. By reducing vulnerability, the potential risk to an asset is also reduced.

2. Assessing Vulnerability

a. Installation or unit AT officers conduct a VA using key AT Working Group members in a collaborative effort as the assessment team. Teams should include representation from operations, security, intelligence, counterintelligence, law enforcement, communications, fire department, engineers, medical services, housing, emergency planning, and WMD planning and response. The VA must comply with DODD 2000.16.

b. The end-state of the VA process is the identification of physical characteristics or procedures that render critical assets, areas, or special events vulnerable to a range of known or feasible terrorist capabilities. Determination of vulnerability is partly a function of the commander's desired level of protection for the asset, area, or special event. Although performing a detailed VA is not simple, the results quantifying and rating the effectiveness of an installation's current protective measures are invaluable and provide a major tool for developing AT countermeasures. The VA methodology should follow the below sequence:

(1) List assets and the threats against those assets.

(2) Determine criteria to be used to assess assets against.

(3) Train assessment team on assessment intent and methodology.

(4) Assessment Team conducts assessment.

(5) Consolidate and review assessment results.

c. The Department of Defense has created several tools to assist conducting Vulnerability Assessments to include the Joint Staff Core Vulnerability Assessment Management Program (CVAMP); Mission, Symbolism, History, Accessibility, Recognizability, Population, and Proximity (MSHARPP); and Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability (CARVER). The Defense Threat Reduction Agency (DTRA) AT VA Team Guidelines are another excellent tool available for Local (Base) Vulnerability Assessments. This is a comprehensive checklist that is directly linked to DODD 2000.16 AT Standards and produces a product similar to a Joint Staff Integrated VA (JSIVA).

3. Suggested VA Methodologies

a. Facility Commanders are encouraged to use a risk assessment tool that is simple yet has some quantifiable logic to help in decision making. Assessment teams shall use the methodology to determine terrorist options against specific targets and use them as examples of protection strategies discussed in this appendix. The suggested tools offered below have their strengths and their weaknesses - as with all tools, there is a right tool for the job at hand. As an example, CARVER is not specifically tailored for AT assessments, although it can be used. Likewise, MSHARPP is a targeting analysis tool geared more closely to assessing personnel vulnerabilities. Assessment team members should be cognizant of potential gaps when choosing one methodology over another. The use of the Joint Staff CVAMP shall assist commanders and ATOs in managing their command's vulnerabilities and associated funding requirements.

b. MSHARPP.

(1) The purpose of the MSHARPP 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 section provides an example of how to use MSHARPP.

(2) After developing a list of potential targets, use the MSHARPP selection factors to assist in further refining your assessment by associating a weapon/tactic to a potential target to determine the efficiency, effectiveness and plausibility of the method of attack and to identify vulnerabilities related to the target. After the MSHARPP values for each target or component are assigned, the sum of the values indicates the highest value target (for a particular mode of attack) within the limits of the enemy's known capabilities.

(3) Mission. 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.

(a) When assessing points in this area, determine whether or

not an attack on mission components shall cause degradation by assessing the Component's:

1. Importance. Importance measures the value of the area or assets located in the area, considering their function, inherent nature, and monetary value.

2. Effect. Effect measures the ramifications of a terrorist incident in the area, considering the psychological, economic, sociological, and military impacts.

3. Recuperability. Recuperability 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.

(b) Mission Criteria Scale. 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.

1. ONE. Destroying or disrupting this asset would have no effect on the ability of the installation to accomplish its mission.

2. TWO. The installation could continue to carry out its mission if this asset were attacked, albeit with some degradation in effectiveness.

3. THREE. Half of the mission capability remains if the asset were successfully attacked.

4. FOUR. Ability to carry out a primary mission of the installation would be significantly impaired if this asset were successfully attacked.

5. FIVE. Installation cannot continue to carry out its mission until the attacked asset is restored.

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

(a) High profile, direct symbol of target group or ideology, asset is perceived to be vital to the mission of the installation.

(b) Low profile, direct symbol of target group or ideology.

(c) Low profile and/or obscure symbol of target group or

ideology.

(5) History. Do terrorist groups have a history of attacking this type of target? While you must consider terrorist trends worldwide, focus on local targeting history and capabilities. Symbolism criteria scale:

(a) Strong history of attacking this type of target.

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

(c) Little to no history of attacking this type of target.

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

(a) The four basic stages to consider, when assessing accessibility are:

1. Infiltration from the staging base to the target area.

2. Movement from the point of entry to the target or objective.

3. Movement to the target's critical element.

4. Exfiltration.

(b) Accessibility criteria scale.

1. Easily accessible, standoff weapons can be employed.

2. Inside Perimeter fence, climbing or lowering required.

3. Not accessible or inaccessible without extreme difficulty.

(7) Recognizability. A target's recognizability is the degree to which it can be recognized by an operational element and/or intelligence collection and reconnaissance asset under varying conditions. Weather has an obvious and significant impact on visibility (yours and the enemy's). Rain, snow, and ground fog may obscure

observation. Road segments with sparse vegetation and adjacent high ground provide excellent conditions for good observation. Distance, light, and season must be considered. 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. Recognizability criteria scale:

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

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

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

(d) Target cannot be recognized under any conditions—except by experts.

(8) Population. Population addresses two factors: quantity of personnel and their demography. Demography 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.

(a) When assessing points in this area, determine whether or not the group(s) have a history of, or are predicted to target:

1. Military personnel.

2. Family members (US citizens in general).

3. Civilian employees of the US Government (include local nationals).

4. Senior officers or other high-risk personnel.

5. Member of an ethnicity (racial, religious, or regionally defined).

(b) Quantity addresses the number of people that would become victims if a particular target were attacked. 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).

(c) Population criteria scale.

1. Densely populated; prone to frequent crowds, facility routinely contains substantial numbers of personnel known to be targeted by the enemy and/or the population is comprised of personnel deemed vital to the accomplishment of the installation's mission.

2. Relatively large numbers of people, but not in close proximity (i.e., spread out and hard to reach in a single attack), contains known target group, but rarely in large concentrations, population has no special segment necessary for mission accomplishment.

3. Sparsely populated; prone to having small groups or individuals, little target value based on demographics of occupants.

(9) Proximity. Is the potential target located near other personnel, facilities, or resources that, because of their intrinsic value or "protected" status and a fear of collateral damage, afford it some form of protection? (e.g., near national monuments, protected/religious symbols, etc., that the enemy holds in high regard).

(a) 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.

(b) Proximity criteria scale.

1. Target is isolated; no chance of unwanted collateral damage to protected symbols or personnel.

2. Target is in close enough proximity to place protected personnel, facilities, etc., at risk of injury or damage, but not destruction.

3. Target is in close proximity; serious injury/ damage or death/total destruction of protected personnel/facilities likely.

(10) In an 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 MSHARPP analysis must consider both the present force protection posture and enhanced postures proposed for escalating FPCONs. 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.

c. CARVER.

(1) CARVER is a very useful tool for determining that your critical assets might indeed offer an enemy a good or soft target. If you employ the very same CARVER analysis to every asset, it shall yield a good estimate as to the attractiveness of those assets to an enemy. Specifically commanders shall then know which "targets" require hardening or otherwise increased protection.

(2) CARVER is an acronym, with each letter representing the following:

(a) Criticality. The importance of a system, subsystem, complex, or component. A target is critical when its destruction or damage has a significant impact on the output of the targeted system, subsystem, or complex, and at the highest level, on the unit's ability to make war or perform essential functions. Criticality depends on several factors:

1. How rapidly shall the impact of asset destruction affect the unit's essential functions.

2. What percentage of output and essential functions is curtailed by asset damage.

3. Is there an existence of substitutes for the output product or service.

4. What is the number of assets and their position in the system or complex flow diagram.

5. Criticality asks the question: How critical is the asset to your mission accomplishment?

(b) Accessibility. The ease that an asset can be reached, either physically or by standoff weapons. An asset is accessible when a terrorist element can physically infiltrate the asset, or the asset can be hit by direct or indirect fire. As a reminder, assets can be people, places, or things. The use of standoff weapons should always be considered when evaluating accessibility. Survivability of the attacker is usually most related to a target's accessibility. Accessibility asks the question: How easily can an enemy get access to, or have their weapons reach the asset?

(c) Recuperability. A measure of time required to replace, repair or bypass, the destruction or damage inflicted on the target. Recuperability varies with the sources and ages of targeted components and with the availability of spare parts. The existence of economic embargoes and the technical resources of the installation shall influence recuperability. Recuperability asks the question: How long would it take you to repair or replace the asset?

(d) Vulnerability. A measure of the ability of the terrorist to damage the target using available assets (people and material). A target (asset) is vulnerable if the terrorist has the means and expertise to successfully attack it. Vulnerability depends on:

1. The nature of the construction of the target.

2. The assets available (manpower, transportation, weapons, explosives, and equipment) to defend the asset.

3. Vulnerability asks the question: Is the asset literally hardened or guarded? Are measures in place to mitigate any threat?

(e) Effect on the population. The positive or negative influence on the population as a result of the action taken. Effect considers public ~~relation~~ reaction in the vicinity of the target, but also considers the domestic and international reaction as well. Shall reprisals against friendlies result? Shall national PSYOP themes be contradicted or reinforced? Shall exfiltration and evasion be helped or hurt? Shall the enemy population be alienated from its government, or shall it become supportive of the government. Effect is often neutral at the tactical level. Effect asks the question: What is the effect on the local population, be it terror or demoralization, and associated mission degradation?

(f) Recognizability. The degree that a target can be recognized under varying weather, light, and seasonal conditions without confusion with other targets or components.

1. Factors that influence recognizability include the size and complexity of the target, the existence of distinctive target signatures, and the technical sophistication and training of the terrorists.

2. Recognizability asks the question: Can the enemy recognize the target for what it truly is and its importance?

(3) Target selection requires detailed intelligence and thorough planning, and is based on the CARVER factors identified above. The CARVER Matrix is a decision tool for rating the relative desirability of potential targets and for wisely allocating attack resources. Two rules of thumb apply for completing the matrix:

(a) For strategic level analysis, list systems and subsystems.

(b) For tactical level analysis list complexes or components of subsystems and complexes. Keep in mind that the scale can be adjusted, such as one to ten or 10 to 100, provided that consistency is observed.

(4) After completing the matrix for all assets, total the scores and then

rank order those totals to prioritize vulnerabilities.

(5) The following are basic mitigation tips to address four of the six CARVER Components:

(a) Reduce criticality. As practicable have a back-up device, system or tested plan to afford mission accomplishment without the asset; create redundancy either physically or operationally; have a tested and viable Continuity Of Operations Plan; and have a fall-back site for conducting the same mission from another location.

(b) Reduce accessibility. Reduce access both, physical and cyber, as applicable; use barriers, other barricades, carefully controlled pedestrian and vehicle movement and/or access and parking; and use fences, remote motion sensors, and remote video surveillance.

(c) Reduce vulnerability. Harden the structure and/or immediate environment to include window treatment to prevent glass shards, structural reinforcement, and shatterproof and fireproof building materials. Move vehicle parking and access sufficiently away from personnel massing facilities.

(d) Reduce recognizability. Delete location and purpose of facility from all base maps and remove building signs that describe function or give title of unit in facility. Instruct telephone operators to not give out number or existence of facility. Use plant cover, including trees and bushes, to partially conceal facility, particularly from roads.

d. Core Vulnerability Assessment Management Program.

(1) CVAMP is an automated and web-based means of managing a command's vulnerabilities and associated funding requirements. CVAMP key capabilities include:

(a) Provide a means to ~~database~~ enter vulnerability assessment findings into a database in accordance with DODD 2000.16, for both higher headquarters and local assessments.

(b) Provide capability of receiving observations directly from the JSIVA Information System.

(c) Document a commander's risk assessment decision for each vulnerability.

(d) Track the status of known vulnerabilities until mitigated.

(e) Provide a tool to assist in prioritizing vulnerabilities via a

weighted scale based on user input.

(f) Provide commanders a vehicle to identify requirements to the responsible chain of command.

(g) Provide the ability to roll vulnerability data into a resource requirement. This includes unfunded requirement (UFR) submissions as well as emergent and emergency CbT RIF requests. Use of CVAMP is mandatory for submission to the Joint Staff of CbT RIF requests.

(h) Provide ability to control release of vulnerabilities and associated funding requests through the chain of command – access is limited to a "need to know" basis as determined by system administrators at each command level.

(i) Allow for prioritization of emergent CbT RIF requests and UFRs as well as provide a tool to assist in this process based on user input.

(j) Provide a ready reference to track the status of installations and activities by FPCON and/or Terrorism Threat Level.

(2) Registration for CVAMP is embedded within the Joint Staff's Antiterrorism Enterprise Portal via the SIPRNET. Once registered on ATEP, system administrators identified at each level of command shall assign CVAMP roles and functions to users based on their needs/requirements. To allow for flexibility, administrators can assign multiple roles to a user. Each role sets specific user permissions within the system. Besides SIPRNET access, minimal additional equipment or training is required to use CVAMP. The system operates in a user-friendly format with drop down menus and no complex computer skills are required to create, review, modify or manage the program. Initial CVAMP-related roles and their permissions are:

(a) Commander. Capability to read and/or write with comment and retains sole release authority to higher headquarters on all vulnerability assessments, vulnerabilities, and funding requests.

(b) ATO. Capability to create vulnerability assessments, vulnerabilities and funding requests.

(c) Resource Manager. Capability to read and/or write to all funding requests.

(d) Assessor. Capability to create observations associated with a vulnerability assessment.

(e) System Administrator. Capability to assign and manage roles within immediate organization and one level down.

(f) Users should contact their local/and or next higher headquarters CVAMP administrators to establish their roles within CVAMP.

Intentionally Blank

APPENDIX C
CRITICALITY ASSESSMENT

1. General

This appendix describes the methodology commanders and civilian equivalents can use to complete a Criticality Assessment. A critical asset is a specific entity that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation to continue to function effectively. ~~any facility, equipment, service or resource considered essential to DOD operations in peace, crisis, and war and warranting measures and precautions to ensure their continued efficient operation; protection from disruption, degradation or destruction; and timely restoration.~~ Both regulations and the commander's priorities and intent determine critical assets. Regulations cover items such as VIPs, ammunition storage areas, etc. The Commander's intent extends coverage to other items such as mission critical and high occupancy assets. Critical assets can be people, property, equipment, activities and operations, information, facilities, and materials.

2. Conducting the Criticality Assessment.

a. The Criticality Assessment identifies assets supporting DOD missions, units, or activities and deemed critical by military commanders or civilian agency managers. For AT purposes, the Criticality Assessment should include high-population facilities, which may not necessarily be mission essential (recreational activities, theaters, or sports venues). It addresses the impact of temporary or permanent loss of assets. It examines costs of recovery and reconstitution including time, dollars, capability and infrastructure support.

b. In military units deployed under the command of the Services or a combatant command, the staff at each command echelon determines and prioritizes critical assets. The commander responsible for AT approves the prioritized list.

The Criticality Assessment goals are:

(a) Identify installation's/unit's key assets.

(b) Determine whether critical functions can be duplicated under various attack scenarios.

(c) Determine time required to duplicate key assets or infrastructures efforts if temporarily or permanently lost.

(d) Determine priority of response to key assets, functions, and infrastructures in the event of fire, multiple bombings, or other terrorist acts.

c. The assessment process described below is specifically designed for AT Assessment and Planning. Other DOD processes, such as the "Mission Essential Vulnerable Area" (MEVA), the "Mission, Symbolism, History, Accessibility, Recognizability, Population, and Proximity" (MSHARPP) methodology, and the "~~Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability~~" (~~(~~CARVER~~)~~ matrix tool, offer similar types of subjective assessments but are not specifically tailored for antiterrorism assessments. While the MSHARPP and CARVER processes are optional methodologies for those who are familiar with their use, both have design limitations and are best used only as an adjunct to the risk assessment (combination of the criticality, threat, and vulnerability assessment ratings) and management methodology.

d. The purpose of the Criticality Assessment process is to identify and prioritize all assets on an installation. ~~Assets include personnel, equipment, stockpiles, buildings, recreation areas, or transportation systems that are deemed critical as defined by *DoD Antiterrorism Force Protection Installation Planning Template*.~~ Assets include personnel, equipment, stockpiles, buildings, or transportation systems that are deemed critical as defined by *DODD 3020*. There are many different types of assets critical to mission accomplishment and it is important not to exclude some assets because they are not necessarily mission-essential or physically located on the installation. For example, a telephone switching facility located off base may be essential to communications if alternative systems are not identified. There may also be assets on the installation which are not critical to the direct operation of the installation, but are critical to the Department of Defense.

e. It may also be useful to link identified threat attack means to a specific time period or location. For example, a terrorist group operating in the proximity of the installation may typically target areas, such as schools or the commissary and/or exchange that contain a large number of people at certain times.

f. When determining asset criticality, use of the following criteria shall assist in standardizing the process.

(1) Importance. Measures the value of the area or assets located in the area, considering their function, inherent nature, and monetary value.

(2) Effect. Measures the ramification of a terrorist incident in the area, considering the psychological, economic, sociological, and military impacts.

(3) 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. Even if a DOD asset is injured, damaged, or destroyed, it may have future value in the accomplishment of other DOD missions or be of great symbolic value to the Department of Defense, the US Government, and the American people. Consideration should therefore be given to the resources that must be

expended to recover an asset and in some cases, repair it for return to service with the Department of Defense in the future.

(4) Mission Functionality. Measures key positions, special facilities, specialized equipment, etc., used to fulfill assigned missions.

(5) Substitutability. Are there substitutes available for personnel, facilities or materiel? Can assigned missions be performed using substitutes? If the substitutes are less capable, can the mission still be accomplished successfully?

(6) Reparability. If a DOD asset is injured or damaged, can it be repaired and rendered operable? How much time is required? How much would it cost? Could repairs be accomplished in a timely manner? Would repairs degrade asset performance, and if so, can the mission be accomplished in the degraded condition?

3. Criticality Assessment Matrix.

a. The purpose of a Criticality Assessment Matrix is to determine the criticality of each asset, which shall also help to prioritize them. For each asset, the Assessment Team shall assign values for each criteria based on a scale, such as one to ten. The Assessment Team must determine what criteria to use.

b. Once all asset values are tallied, they can be rank-ordered such that highest score is "most critical" and lowest score is "least critical." However, it is important to emphasize that not all assets in the matrix shall be "essential for mission accomplishment".

Intentionally Blank

APPENDIX D
SAMPLE ANTITERRORISM PLAN FORMAT

1. Overview

a. The format outlined below is offered as one means of developing an AT plan. It is optimized for a base or installation, but can be adapted for other facilities and deployed units. It is meant to help the AT officer structure the AT plan in a comprehensive and organized manner. The format is patterned after the standard five-paragraph military operations order (Situation-Mission-Execution-Administration and Logistics-Command and Signal).

b. This format enables the synchronization of existing programs such as Law Enforcement, Physical Security, AT, OPSEC, INFOSEC, High-Risk Personnel protection, and other installation efforts. AT Plans should be integrated into all plans and separate annexes. Remember that staff interaction is a crucial element of developing a realistic, executable plan.

c. Although this sample is patterned after the military operations order, it ~~is applicable~~ applies to managers of ~~OSD~~ Defense Agencies and DOD field activities as they develop plans to protect personnel, activities, and material under their control.

d. This sample uses supporting Annexes, Appendices, Tabs, and Enclosures to provide amplifying instructions as required. This method shortens the length of the basic plan (which should be read by all personnel outlined in the plan), and provides organization, structure, and scalability.

Installation/Operation Name
Location
Date/Time Group

INSTALLATION/OPERATION NAME ANTITERRORISM PLAN 2002 (AT-04)

Task Organization. [Include all agencies/personnel (base and civilian) responsible to implement the plan. Include as a separate Annex. See Annex A (Task Organization).]

Maps/Charts: [List all applicable maps or charts. Include enough data to ensure personnel are using the correct year/edition/version of the subject material.]

Time Zone: [Enter the time zone of the installation. Indicate the number of hours to calculate (plus/minus) ZULU time.]

Ref: [Enter the compilation of pertinent publications, references, MOU/MOA~~/MAA~~. This list may be included in a separate Annex. See Annex Q (References).]

1. SITUATION

a. General. [This plan applies to all personnel assigned or attached to the installation. [Describe the political/military environment in sufficient detail for subordinate commanders, staffs, and units to understand their role in the installation AT operations.]

b. Enemy. [The enemy is any adversary capable of threatening the installation's personnel, facilities, and equipment. ~~[(ENTER t~~The general threat of terrorism to this installation including the intentions and capabilities, identification, composition, disposition, location, and estimated strengths of hostile forces. Include the general threat of terrorist use of WMD against this installation. This information should remain unclassified when possible. See paragraph 1f, Intelligence, on identifying specific threats.~~]~~ .) This information may be included as a separate Annex. See Annex B (Intelligence).]

c. Friendly. [~~ENTER t~~The forces available (both military and civilian) to respond to a terrorist WMD attack. Include the next higher headquarters and adjacent installations, and any units/organizations that are not under installation command, but may be required to respond to such an incident. These units / organizations may include Host Nation (HN) and US military police forces, fire and emergency services, medical, and federal/state and local agencies, special operations forces, engineers, detection (radiological, nuclear, biological, and chemical) decontamination or smoke units, and explosive ordnance disposal (EOD). Include MOAs/MOUs and any other special arrangements that will improve forces available to support the plan. If in the ~~U.S.~~US and its territories, the Department of Justice, Federal Bureau of Investigation (FBI) is responsible for coordinating all Federal agencies and DOD forces assisting in the resolution of a terrorist incident. If outside the ~~U.S.~~US and its territories, the Department of State (DOS) is the lead agency. This information can be included in a separate Annex(s). See Annex A (Task Organization) and Annex J (Command Relationships).]

d. Attachments/Detachments. [~~ENTER i~~Installation/civilian agencies NOT normally assigned to the installation that are needed to support this plan. Explain interagency relationships and interoperability issues. This can be listed in other Annexes. See Annex A (Task Organization) and Annex J (Command Relationships).]

e. Assumptions. (List planning/execution assumptions) [~~ENTER a~~All critical assumptions used as a basis for this plan. Assumptions are those factors unlikely to change during the implementation of the AT plan and that must addressed in order to continue to plan. They can range from the installation's troop strength to addressing the local political/social environment. Examples follow:

(1) The installation is vulnerable to theft, pilferage, sabotage, and other threats. The installation is also vulnerable to a WMD attack.

(2) An act of terrorism involving WMD can produce major consequences that will overwhelm almost immediately the capabilities of the installation.

(3) Security personnel, both military and civilian, may be insufficient to provide total protection of all installation resources; therefore, the principal owner or user of a facility, resource, or personnel must develop adequate unit awareness and safeguard measures.

(4) No single unit on the installation possesses the expertise to act unilaterally in response to WMD attacks.

(5) If protective equipment is not available, responders will not put their own lives at risk.

(6) Local, non-military response forces will arrive within [time] of notification.

(7) Units specializing in WMD response will arrive on-site within [number of hours based on installation location] of notification.

(8) The HN is supportive of ~~U.S.~~US policies, and will fulfill surge requirements needed to respond to a WMD incident IAW MOAs/MOUs.]

f. Intelligence. [~~ENTER t~~ The person, staff, or unit responsible for intelligence collection and dissemination. The installation commander must have a system in place to access current intelligence. This can be included in Annex B (Intelligence).] [National-level agencies, Combatant Commanders, and intelligence systems provide theater or country threat levels and threat assessments. In the ~~U.S.~~US and its territories, local installations must obtain the local terrorist threat information by querying the FBI through the installation's law enforcement liaison, local law enforcement, or other federal agencies.]Obtain these assessments, as they will serve as a baseline for the installation's tailored assessment. The installation should have a process in place for developing the installation's tailored threat assessment or "local threat picture." The installation's tailored threat assessment should be continuously evaluated, updated, and disseminated, as appropriate, and as directed by the installation commander. The commander should determine the frequency and the means of dissemination of the installation's tailored AT product. Note: Commanders cannot change the threat level, which is developed at the national-level although they can declare higher Force Protection Conditions (FPCONs) than the baseline.

2. MISSION. [~~ENTER a~~ A clear, concise statement of the command's mission and the AT purpose or goal statement supporting the mission. The primary purpose of the AT plan is to safeguard personnel, property, and resources during normal operations. It is also designed to detect and deter a terrorist threat, enhance security and AT awareness, and to assign AT responsibilities for installation personnel.]

3. EXECUTION

a. Commander's Intent. (Commander's vision on how he/she sees the execution of the unit's AT program. Refer to Service planning doctrine for assistance.)

b. Concept of Operations. [~~ENTER h~~ How the overall AT operation should progress. This plan stresses deterrence of terrorist incidents through preventive and response measures common to all combatant commands and Services. During day-to-day operations, the installation should stress continuous AT planning and passive, defensive operations. This paragraph should provide subordinates sufficient guidance to act if contact or communications with the installation chain of command is lost or disrupted.]

(1) The installation's AT Concept of Operations should be phased in relation to pre-incident actions and post-incident actions. AT planning and execution requires that staff elements work with a much greater degree of cohesiveness and unity of mission than that required during the conduct of normal base sustainment operations. The AT mission, and the unpredictability of its execution, requires

very specific "how to" implementation instructions of DOD FPCON Measures and in what manner these actions must be coordinated. This "how to" element is not normally included in the Concept of Operations paragraph; however the necessity to provide "how to" guidance in the AT plan requires a different manner of data presentation to ensure brevity and clarity. The implementation instructions are put into the form of action sets and can be displayed in the form of an execution matrix (Pre-Incident Action Set Matrix).

(2) In Post-Incident planning, the installation should focus on its response and reconstitution responsibilities upon notification of a terrorist incident and the procedures for obtaining technical assistance/augmentation if the incident exceeds the installation's organic capabilities. National-level responders (Federal Emergency Management Agency (FEMA), Red Cross, and Federal Bureau of Investigation (FBI)) may not be immediately accessible or available to respond to an installation's needs. Therefore each installation must plan for the worst-case scenario, by planning its response based on its organic resources and available local support through MOA/MOUs.

(3) The situation may dictate that the installation not only conduct the initial response but also sustained response operations. Many installations do not have onboard WMD officers or response elements. This paragraph will include specific implementation instructions for all functional areas of responsibility and the manner in which these actions must be coordinated. The implementation instructions can be put in the form of actions sets and displayed in the form of a synchronization matrix (Post-Incident Action Set Synchronization Matrix). The synchronization matrix format clearly describes relationships between activities, units, supporting functions, and key events which must be carefully synchronized to minimize loss of life and to contain the effects of a terrorist incident.

c. Tasks. [~~ENTER t~~ The specific tasks for each subordinate unit or element listed in the Task Organization paragraph. Key members of the installation have responsibilities that are AT and/or WMD specific. The commander should ensure that a specific individual/unit/element within the installation is responsible for each action identified in this plan. Each individual/unit/element must know the tasks and responsibilities, what these responsibilities entail, and how these will be implemented. While the tasks and responsibilities for each AT planning and response Element will be delineated in the Pre- and Post-incident Action Set Matrices, it is recommended that the installation commander identify/designate the primary lead for each element and enter that information in this paragraph.]

(1) First Subordinate Unit/Element/Tenant

(a) Task listing.

d. Coordinating Instructions. [This paragraph should include AT specific coordinating instructions and subparagraphs, as the commander deems appropriate. In addition, this section of the AT plan outlines aspects of the installation's AT posture that require particular attention to guarantee the most effective and efficient implementation of the AT plan. For the purposes of this plan, there are five basic coordinating instructions: 1) AT planning and response elements; 2) Procedural; 3) Security Posture; 4) Threat Specific Responsibilities; and 5) Special Installation Areas. The reader will be directed to specific Annexes that will provide amplifying instructions on these topics. The sections listed below are representative, and may not be all-inclusive.

(1) AT Planning and Response. For instructional purposes, this template outlines AT planning and response elements on the installation required to respond to a terrorist/WMD incident. Initial and sustained response to an attack must be a coordinated effort between the many AT planning and response elements of the installation, based on the installation's organic capabilities. As the situation exceeds the installation's capabilities, it must activate MOAs/MOUs with the local/State/ Federal agencies (~~U.S.~~US and its territories) or HN (outside the ~~U.S.~~US and its territories). For the purposes of this plan, an installation's capability is divided into AT planning and response elements. These tailored, installation-level elements parallel the national-level FEMA ESFs and the JSIVA evaluation criteria to the greatest degree possible.

AT Planning & Response Elements

Information & Planning *
Communications * +
HAZMAT *
Security * +
Explosive Ordnance Disposal (EOD) +
Firefighting * +
Health & Medical Services * +
Resource Support *
Mass Care *
Public Works *
Intelligence Process +
Installation AT Plans/Programs +
Installation Perimeter Access +
Security System technology +
Executive Protection +
Response & Recovery +
Mail Handling +

* Derived from FEMA ESFs
+ Derived from JSIVA assessment criteria

(2) Procedural

(a) Alert Notification Procedures. See Appendix 14 to Annex C (Operations).

(b) Use of Force/Rules of Engagement. See Annex H (Legal).

(c) Installation Training & Exercises. See Annex N (AT Program Review, Training & Exercises).

(d) Incident Response. See Appendix 1 to Annex C (Operations).

(e) Consequence Management. See Appendix 1 to Annex C (Operations).

(f) High-Risk Personnel Protection Procedures. See Appendix 9 to Annex C (Operations).

(g) AT Program Review (See Annex N (AT Program Review, Training & Exercises).

(h) Higher Headquarters Vulnerability Assessments. See Annex N (AT Program Review, Training & Exercises).

(3) Security Posture Responsibilities

(a) Law Enforcement. See Appendix 7 to Annex C (Operations).

(b) Physical Security to include Lighting, Barriers, Access Control. See Appendix 6 to Annex C Operations).

(c) Other On-site Security Elements. See Appendix 8 to Annex C (Operations).

(d) Operations Security. See Appendix 10 to Annex C (Operations).

(e) Technology. See Appendix 15 to Annex C (Operations).

(f) EOC Operations. See Appendix 12 to Annex C (Operations)

(g) Critical Systems Continuity of Operations (optional). See Appendix 13 to Annex C (Operations).

(h) Other

(4) Threat Specific Responsibilities

(a) Antiterrorism. See Appendix 2 to Annex C (Operations).

(b) Weapons of Mass Destruction. See Appendix 5 to Annex C (Operations).

(c) Special Threat Situations. See Appendix 3 to Annex C (Operations).

(d) Information Security. See Appendix 11 to Annex C (Operations).

(e) Natural/Man-made Hazards (Optional). See Appendix 16 to Annex C (Operations).

(f) Other

(5) Special Security Areas

(a) Airfield Security. See Appendix 4 to Annex C (Operations).

(b) Port Security. See Appendix 4 to Annex C (Operations).

(c) Embarkation/Arrival Areas. See Appendix 4 to Annex C (Operations).

(d) Buildings. See Appendix 4 to Annex C (Operations).

(e) Other

4. ADMINISTRATION AND LOGISTICS. [~~ENTER t~~The administrative and logistics requirements to support the AT plan, which should include enough information to make clear the basic concept for planned logistics support. Ensure the staff conducts logistical planning for both pre- and post-incident measures addressing the following: locations of consolidated WMD defense equipment; expedient decontamination supplies; Individual Protective Equipment exchange points; special contamination control requirements; retrograde contamination monitoring sites; WMD equipment/supply controlled supply rates and pre-stockage points; and procedures for chemical defense equipment "push" packages. Specific logistics and administrative requirements will emerge throughout the planning process outlined in the Concept of Operations, specifically when developing the action sets. These requirements should be incorporated into this paragraph. Finally, include fiscal instructions on how to support AT operations.

a. Administration. See Annex O (Personnel Services).

b. Logistics. See Annexes D (Logistics) and E (Fiscal).

5. COMMAND AND SIGNAL. [~~ENTER i~~Instructions for command and operation of communications-electronics equipment. Identify the primary and alternate locations of the command post and emergency operations center. Enter the installation's chain of command. Highlight any deviation from that chain of

command that must occur as a result of a WMD incident. The chain of command may change based on the deployment of a Joint Task Force or a President or Secretary of Defense ~~National Command Authority~~-directed mission. Identify the location of any technical support elements that could be called upon in the event of a terrorist WMD incident and the means to contact each. Recommend the installation coordinate with higher headquarters to establish procedures to allow for parallel coordination to report a terrorist WMD incident. The installation must provide for prompt dissemination of notifications and alarm signals, and the timely/orderly transmission and receipt of messages between elements involved in and responding to the incident.]

a. Command. See Annex A (Task Organization) and Annex J (Command Relationships).

b. Signal. See Annex K (Communications).

c. Command Post Locations

(1) Primary: [~~ENTER~~ location]

(2) Alternate: [~~ENTER~~ Location]

d. Succession of Command

(1) First alternate: [~~ENTER~~ POSITION/TITLE]

(2) Second alternate: [~~ENTER~~ POSITION/TITLE]

//SIGNATURE//
Commanding General/Officer
Signature Block

ANNEXES: (Should provide amplifying instructions on specific aspects of the plan. Each ANNEX can be subdivided into APPENDICES, TABS, and ENCLOSURES as required to provide amplifying instructions. Further, some of these supporting documents may be established in other unit operating orders/procedures, and referenced as required.)

ANNEX A - Task Organization [~~ENTER~~ key AT organization composition i.e., AT Working Group, Crisis Management Team, Emergency Operations Center, First Response Elements, etc.]

Appendix 1 – DIA Threat Assessment or Service Worldwide Threat Assessment (e.g., USAF () Postulated Worlwide Nonnuclear Threat)

Appendix ~~1~~ 2 – Table of Organization

Appendix ~~2~~ 3 – Post Prioritization Chart

ANNEX B – Intelligence [~~ENTER~~ the agency(s) responsible for intelligence and specific instructions. In the ~~U.S.~~US and its territories, commanders must obtain the local terrorist threat information by querying the FBI through the installation's law enforcement liaison, local law enforcement or other federal agencies]

Appendix 1 – Local Threat Assessment

Appendix 2 – Local WMD Assessment

Appendix 3 – Local Criticality/Vulnerability Assessment

Appendix 4 – Risk Assessment

Appendix 5 – Pre-deployment AT Vulnerability Assessment

ANNEX C – Operations [This is the most IMPORTANT part of the plan]. Annex C and supporting Appendices will provide specific instructions for all the various AT operations. All other Annexes/Appendices support the implementation of Annex C.

Appendix 1 – Incident Planning and Response [~~ENTER~~ how the various agencies (military/civilian) and resources will be integrated to respond to the operations outlined below. These instructions should be generic enough to apply across the operational spectrum. Specific instructions for each operation will be detailed in the appropriate Annex/Appendix/Enclosure.]

Tab A – Incident Command and Control Procedures
Tab B – Incident Response Procedures
Tab C – Consequence Management Procedures

Appendix 2 – Antiterrorism

Tab A - Mission Essential Vulnerable Assets (MEVA)
Tab B - Potential Terrorist Targets
Tab C – FPCON
Enclosure 1 - FPCON Action Sets [Who/What/When/Where/How]
Tab D - Random Antiterrorism Measures (RAM) Procedures

Appendix 3 - Special Threat Situations

Tab A - Bomb Threats
Enclosure 1 – Bomb Threat Mitigation
Enclosure 2 – Evacuation Procedures
Enclosure 3 – Search Procedures
Tab B - Hostage Barricaded Suspect
Tab C – Mail Handling Procedures

Appendix 4 – Special Security Areas

Tab A – Airfield Security
Tab B – Port Security
Tab C – Embarkation/Arrival Areas.
Tab D – Buildings

Appendix 5 – Weapons of Mass Destruction (CBRNE) & HAZMAT [~~ENTER~~ the specific procedures planning, training, and response to WMD (CBRNE) incidents. Care should be taken to integrate existing plans for response to HAZMAT incidents to avoid duplication. Include "baseline" preparedness.]

Tab A - WMD Action Set Synchronization Matrix [Who/What/Where/When/How]
Tab B – CBRNE Emergency Responder Procedures

Appendix 6 – Physical Security

Tab A – Installation Barrier Plan [~~ENTER~~ procedures and pictorial representation of barrier plan.]
Tab B – Installation Curtailment Plan
Tab C – Construction Considerations
Tab D – Facility and Site Evaluation and/or Selection
Tab E – AT Guidance for Off-Installation Housing

Appendix 7 – Law Enforcement

Tab A – Organization, training, equipping of augmentation security forces
Tab B – Alternate Dispatch Location
Tab C – Alternate Arming Point

Appendix 8 – Other On-Site Security Forces

Appendix 9 – High Risk Personnel

Tab A – List of High Risk Billets

Appendix 10 – Operations Security

Appendix 11 – Information Security

Appendix 12 – Emergency Operations Center (EOC) Operations [~~ENTER~~ procedure for the activation & operations of the EOC.]

Tab A – EOC Staffing (Partial/Full)
Tab B – EOC Layout
Tab C – EOC Messages & Message Flow
Tab D – EOC Briefing Procedures
Tab E – EOC Situation Boards
Tab F – EOC Security and Access Procedures

Appendix 13 – Critical Systems Continuity of Operations Plans (Optional) [~~ENTER~~ those systems that are essential to mission execution and infrastructure support of the installation i.e., utilities systems, computer networks, etc. This document outlines how the installation will continue to operate if one or more critical systems are disrupted or fails and how the systems will be restored.]

Tab A – List of installation critical systems
Tab B – Execution checklist for each critical system

Appendix 14 - Emergency Mass Notification Procedures [~~ENTER~~ the specific means and procedures for conducting a mass notification. Also covered should be the procedures/means for contacting key personnel and agencies.

Tab A – Situation Based Notification
Tab B – Matrix List of Phone Numbers/Email Accounts

Appendix 15 – Exploit Technology Advances [~~ENTER~~ the process and procedures for developing and employing new technology. Identify who is responsible and what should be accomplished.]

Appendix 16 – Higher Headquarters Vulnerability Assessments [~~ENTER~~ procedures for conducting higher headquarters vulnerability assessments.

Appendix 17 – Natural/Man-made Hazards (Optional) [Hurricanes, Flooding, Chemical Plants etc.]

Tab A - Locality specific natural and man-made hazards)

ANNEX D – Logistics (Specific logistics instructions on how to support AT operations)

Appendix 1 – Priority of Work [~~ENTER~~ the priority of employing scarce logistical resource.]

Appendix 2 – Emergency Supply Services

Appendix 3 – Weapons and Ammunition Supply Services

Appendix 4 – Emergency Equipment Services

Appendix 5 – Evacuation Shelters

Appendix 6 – Generator Refueling Matrix

ANNEX E – Fiscal (Specific fiscal instructions on how to support AT operations from pre-incident through post-incident)

Appendix 1 – AT Program of Memorandum Budget Submission Instruction

Appendix 2 – Combating Terrorism Readiness Initiative Fund (CbT RIF) Submission Instructions

Appendix 3 – Fiscal Management during Exigent Operations

ANNEX F – Tenant Commanders (Specific instructions on how tenant commands/agencies support AT operations)

Appendix 1 – Areas of Responsibility (Pictorial)

ANNEX G – Air Operations (Specific air instructions on how to support AT operations)

Appendix 1 – List of Landing Zones (Used for emergency medical evacuations or equipment/personnel staging areas.)

Appendix 2 – LZ Preparation Procedures

ANNEX H – Legal [~~ENTER~~ the jurisdictional limits of the installation's commander and key staff. Although the Department of Justice, Federal Bureau of Investigation (FBI), has primary law enforcement responsibility for terrorist incidents in the United States, the installation commander is responsible for maintaining law and order on the installation. For outside the continental United States (OCONUS) incidents, the installation commander must notify the HN and the geographic combatant commander; the geographic combatant commander will notify the Department of State (DOS). Once a task force or other than installation support arrives on the installation, the agencies fall under the direct supervision of the local Incident Commander. In all cases, command of military elements remains within military channels. The installation should establish HN agreements to address the use of installation security forces, other military forces, and host-nation resources that clearly delineate jurisdictional limits. The agreements will likely evolve into the installation having responsibility "inside the wire or installation perimeter" and the HN having responsibility "outside the wire or installation perimeter". There may be exceptions due to the wide dispersal of work and housing areas, utilities, and other installation support mechanisms that may require the installation to be responsible for certain areas outside of the installation perimeter.]

Appendix 1 – Jurisdictional Issues

Appendix 2 – Use of Force and/or Rules of Engagement Instructions

Appendix 3 – Pictorial Representation of Installation Jurisdiction

ANNEX I – Public Affairs (Specific PAO instructions on how to support AT operations)

Appendix 1 – Command Information Bureau Organization & Operation

Appendix 2 – Local/Regional Media Contact Information

Annex J – Command Relationships (Provides specific guidance on command relationships and military/civilian interoperability issues during incident command and control).

Appendix 1 – AT Organizational Charts [Crisis Management Team, AT Working Group, First Responder Elements, Incident Command Organization (include civilian and other external agencies).]

ANNEX K – Communications (Specific communications instructions on how to support AT operations. Include systems/procedures for SECURE and NON-SECURE communications means.)

Appendix 1 – Installation AT Communication Architecture

Appendix 2 – Incident Command Communication Architecture

Appendix 3 – EOC Communication Architecture

Appendix 4 – Security Force Communication Architecture

Appendix 5 – Fire Department Communication Architecture

Appendix 6 – Medical Communication Architecture

Appendix 7 – Other Agencies

ANNEX L - Health Services (Specific medical instructions on how to support AT operations)

Appendix 1 - Mass Casualty Plan

Appendix 2 - Procedures for Operating with Civilian Emergency Medical Service and Hospitals

ANNEX M – Safety (Specific safety instructions on how to support AT operations)

ANNEX N – AT Program Review, Training, & Exercises

Appendix 1 – AT Program Review

Tab A – Local Assessments
Tab B – Higher Headquarters Assessments

Appendix 2 – AT Required Training

Appendix 3 – Exercises

ANNEX O – Personnel Services [~~ENTER~~ administrative and personnel procedures required to support the plan i.e., civilian overtime, post-traumatic stress syndrome counseling.]

Appendix 1 – Operating Emergency Evacuation Shelters

ANNEX P – Reports [~~ENTER~~ all the procedures for report submissions & report format.]

Appendix 1 – Reporting Matrix

ANNEX Q – References [~~ENTER~~ all supporting reference materials, publication, regulations etc.]

ANNEX R – Distribution [~~ENTER~~ the list of agencies to receive this plan. Cover plan classification, handling and declassification procedures.]

Intentionally Blank

APPENDIX E
ANTITERRORISM CHECKLIST

1. Introduction.

Protection of DOD assets is an inherent obligation of military commanders. The following ~~C~~checklist is a self-assessment, management tool that can be used by the commander and/or antiterrorism officer to assess the status of his/her AT program. This checklist is structured around the AT Standards outlined in DODI 2000.16. Not all the standards are applicable to all levels of command, therefore, commanders and Service AT guidance should be used where applicable.

YES or NO

2. Questions for Commanders/Managers to Evaluate AT Program Adequacy:

a. Program Review

_____ Is commander/ATO aware of and integrating other programs supporting FP?

_____ Do ALL installation units participate in RAMs?

_____ Is the AT program comprehensive, current, and effective?

_____ Can the unit do the mission under FPCONs in use?

_____ Are critical FPCONs compromised for unit morale or convenience?

_____ ATO staff and resources sufficient, e.g., reliable and accessible SIPRNET access?

_____ Is AT a routine element of daily mission planning and execution?

_____ Are operational patterns varied?

_____ Is OPSEC included in mission planning?

_____ Does the unit continually monitor threat and corresponding security posture?

_____ Does the unit monitor and control access of visitors and employees in sensitive areas?

_____ Has the threat level changed since last VA?

_____ Is the threat assessment current and valid?

_____ Are RAMs having the desired effect on unit awareness, readiness, and deterrence?

_____ Does the unit have an AT program and security posture appropriate for mission and potential threat?

_____ AT Officer appointed?

_____ AT Working Group (ATWG) designated?

_____ DIA, service specific and/or FBI Threat Assessment current?

_____ Vulnerability assessment current?

_____ AT Plan complete?

_____ Program review within past 12 months?

_____ AT Plan exercised within past 12 months?

_____ AT Level I training current?

_____ Have you reviewed DODI 2000.16, *DoOD Antiterrorism Standards*, and appropriate commander / Service AT guidance?

_____ Is commander/Service AT guidance implemented?

b. Organize for AT:

_____ Does unit have adequate focus on AT?

_____ Is unit ATO school trained?

_____ Are right functions represented in ATWG?

_____ Is ATWG active? Meeting minutes documented, open items follow-up and closed? Accomplishments?

c. Threat Assessment:

Do Threat Assessments provided by DIA, service counterintelligence, intelligence and/or FBI integrate with ~~and/or~~ the local threat assessment process:

_____ Identify specific terrorist capabilities, weapons, and tactics (to include WMD)?

_____ Consider the vulnerability of the facilities and utilities?

_____ Consider the criticality of the facilities and utilities?

_____ Provide the necessary information the commander to help tailor FPCONs?

_____ Have a review mechanism to provide up to date information?

_____ Is the unit aware of current and potential threats (conventional and WMD)?

_____ Do you know the DIA and/or FBI (CONUS) assessed threat level for the area?

_____ Has the commander assigned higher local threat level?

_____ Is a formal intel assessment on hand & current?

_____ Relationship with supporting Intel activity?

_____ Is counter-intelligence or law enforcement support needed?

_____ Local information considered?

_____ Local information network established? Part of ATWG?

_____ Aggressive list of threat options identified?

d. Vulnerability Assessment:

_____ Has a local vulnerability assessment been conducted within the past year?

_____ Did the vulnerability assessment identify vulnerabilities and means to eliminate or mitigation them?

_____ Did the vulnerability assessment identify options for enhanced protection of DOD personnel and assets?

Does the AT vulnerability assessment assess the following functional areas at a minimum:

_____ AT Plans and Programs.

_____ Counterintelligence, Law Enforcement, Liaison, and Intelligence Support.

_____ AT Physical Security Measures.

_____ Vulnerability to a Threat and Terrorist Incident Response Measures.

_____ Vulnerability Assessment for Terrorist Use of WMD.

_____ Availability of resources to support plans as written.

_____ Frequency and extent to which plans have been exercised.

_____ Level and adequacy of support from the host nation, local community, and where appropriate, inter-Service and tenant organizations to enhance force protection measures or respond to a terrorist incident.

_____ Status of formal and informal agreements to support AT functions.

_____ Does the vulnerability assessment team contain expertise in order to meet the intent of providing comprehensive assessments?

_____ Is there a process to track and identify vulnerabilities through the chain of command?

e. MOU/MOA

_____ Is unit conforming to and employing MOU/MOA for local support?

_____ Does unit or any detached personnel fall under State Department for force protection?

_____ Are State Department's force protection instructions on hand for those individuals?

_____ Are organizations identified with jurisdiction for law enforcement, health, safety, and welfare of assigned service members on and off duty?

_____ Is unit conforming to jurisdictional agreements in these areas (SOFA, inter-agency)?

_____ Are local community organizations with shared security interests (police, federal law enforcement, hospitals, and public health) identified?

_____ Are mutual aid agreements in place with local community to leverage shared interests?

_____ Have mutual aid agreements been reviewed by higher HQ?

_____ Are mutual aid agreements executable (liability, jurisdiction, capabilities)?

f. Mitigate WMD Effects

_____ Has unit prepared for WMD attack?

_____ Does AT plan consider terrorist use of WMD (CBRNE)?

_____ Does the command have the procedures to process immediately through the chain of command reports of significant information obtained identifying organizations with WMD capability in their ~~AOR?~~ operational area?

_____ Is an estimate of terrorist potential use of WMD indicated in the local threat assessment?

_____ Procedures for detection of unconventional CBRNE attacks?

_____ Does unit training include awareness of indicators of unconventional attacks?

_____ Do all personnel have individual protective equipment available?

_____ Are collective protective systems available?

_____ Is CBRNE detection equipment available?

_____ Is decontamination equipment available?

g. Antiterrorism Plan

_____ Is the AT Plan signed?

_____ Does the installation incorporate AT planning into operations orders for temporary operations or exercises?

_____ Does the plan specify the AT mission and concept of operation?

_____ Does the plan layout the task organization and Mission Essential ~~or~~ Vulnerable Areas (MEVAs)?

_____ Does the plan include the Risk Management process, to include annual AT Threat Assessment with WMD coverage?

_____ Is there a process, based on local terrorism threat information, to raise FPCONs?

_____ Does the plan provide actions at each FPCON?

_____ Are site-specific AT measures, linked to FPCONs classified as a minimum, CONFIDENTIAL?

_____ Is the current FPCON measure adequate for the local threat?

_____ Does the plan provide a baseline for normal ops?

_____ Does plan provide diagram for Random Antiterrorism Measures (RAMs)?

_____ Does the plan include Security Force operations (including augmentation forces) and post priorities?

_____ Has the plan been reviewed within the past year to remediate procedural and resource shortfalls?

_____ Has the plan been approved by higher headquarters (HQ)?

_____ Received/approved AT plans from lower HQ?

_____ Is the plan executable?

_____ Is the plan resourced?

_____ Does the plan mitigate vulnerabilities with policy and procedural solutions?

_____ Does the plan address response to incident and mass casualties?

Does the AT plan contain, as a minimum, site specific procedures for:

_____ Terrorism Threat Assessments?

_____ Vulnerability Assessments?

_____ Program Review?

_____ Training?

_____ AT Physical Security Measures?

_____ Mass notification procedures?

_____ Incident Response Measures?

_____ Consequence Management Measures?

_____ AT considerations for plans/orders for temporary operations or exercises?

Does the command have an adequate "Baseline" security posture to include:

_____ General AT and physical security awareness?

_____ Adequately equipped and trained First Response Forces?

_____ A security posture, capable of sustained operations and commensurate to the local threat, that adequately protects personnel and assets?

_____ Plans and procedures to transition from Normal Operations to an Elevated state of readiness/execution?

_____ Is there a process for you to evaluate subordinate units' and/or tenant commands' knowledge and status of their AT responsibilities?

h. Training and Exercises:

Are personnel receiving the appropriate levels of AT training to include:

_____ Level I-IV training.

_____ Level II training.

_____ Level III training.

_____ Level IV training.

~~_____ High Risk Personnel.~~

_____ AOR specific training prior to deployment.

_____ A system to track and document training.

_____ Is individual awareness of terrorism threat sufficient for threat environment/mission?

~~_____ Annual Level I training current?~~

~~_____ AOR updates current and briefed?~~

_____ Special local individual protective measures briefed and used?

_____ Has the command conducted field and staff training (annually) to exercise AT plans to include?

_____ AT Physical Security measures.

_____ Terrorist Incident Response measures.

_____ Terrorist Consequence Management measures.

_____ FPCON attainment procedures.

_____Does the command maintain exercise AARs/Lessons Learned and document actions taken to remediate identified shortfalls for at least a year?

Does command pre-deployment training include:

_____ Credible deterrence/response.

_____ Deterrence-specific tactics, techniques, and procedures.

_____ Terrorist scenarios and hostile intent decision-making.

i. Antiterrorism Resources:

_____ Does AT resource program support the required long-term security posture?

_____ Defined resource requirements to mitigate security deficiencies?

_____ Requirements justified with risk analysis?

_____ Alternative plans, policy, and procedural solutions considered or implemented?

_____ Does the command have a formal process to track, document, and justify resource requirements and identify resource shortfalls to Higher HQ?

_____ Higher HQ approved these requirements?

_____ Does the command request CbT-RIF for emergent and or emergency commander AT requirements?

~~_____ Emergent (OCONUS) needs submitted for immediate support by CbT-RIF?~~

_____ Does the command incorporate AT requirements into the Program Objective Memorandum (POM) process?

_____ POM requirements submitted for out year support of CbT-RIF funded investments?

_____ Status of CbT-RIF and POM requirements in the program/budget process?

_____ AT and security factors adequately weighed in acquisition and use of facilities (both temporary and permanent)?

_____ Current facilities conform to DOD and Component AT military construction MILCON standards?

_____ Do structural engineers and security personnel work together to incorporate AT consideration in building design and review?

_____ Are DOD AT Standards for buildings incorporated into new constructions?

_____ Is technology being used to enhance security and human performance?

_____ Are technologies being identified as recommended/required for higher threat levels/FPCONs?

_____ Is the AT Officer a member of the Resource Management Committee?

j. ATO Assigned in Writing

_____ Has the commander designated a Level II qualified/trained commissioned officer, non-commissioned officer, or civilian staff officer in writing as the ATO?

_____For deploying organizations (e.g., battalion, squadron, ship) have at least one Level II qualified individual designated in writing?

_____ Has the ATO attended a Service approved Level II AT Training course?

3. Operations Security

_____ Have procedures been established that prevent terrorists from readily obtaining information about plans and operations (e.g., not publishing the commanding general's itinerary, safeguarding classified material, evaluating articles in installation publications)?

_____ Does the plan allow for in-depth coordination with the installation's OPSEC program?

_____ Has an OPSEC annex been included in the contingency plan?

4. Threat Information Collection and Analysis

_____ Has the commander tasked the appropriate organization under his/her

command to gather, analyze, and disseminate terrorism threat information?

_____ Are personnel in the command encouraged and trained to report information on individuals, events, or situations that could pose a threat to the security of DOD personnel, families, facilities, and resources?

_____ Does the command have procedures to receive and process Defense Threat ~~Terrorism~~ Warning Reports Messages and/or higher headquarters threat message?

_____ Does the command have technology to access critical terrorism intelligence e.g., SIPRNET?

5. Threat Information Flow

_____ Does the command forward all information pertaining to suspected terrorist threats, or acts of terrorism involving DOD personnel or assets for which they have AT responsibility up and down the chain of command?

_____ Does the command ensure there is intelligence sharing among all organizations?

_____ Does the command provide tailored threat information for transiting units?

6. Personnel Security

_____ Has the threat analysis identified individuals vulnerable to terrorist attack?

_____ Has a training program been established to educate both military and civilian personnel in the proper techniques of personnel protection and security commensurate with the local threat and the type of position held?

7. Executive Protection and High Risk Personnel Security

_____ Has the command identified high-risk billets and high-risk personnel to higher headquarters annually?

_____ Have personnel designated as "-Personnel at High-Risk to Terrorist Attack" and "Personnel Assigned to High-Risk Billets" received appropriate AT training?

_____ Has the command annually reviewed and revalidated the protective services for executives?

_____ Has the command taken necessary measures to provide appropriate protective services for designated individuals in high-risk billets and high-risk personnel?

_____ Does the command review needs for supplemental security within 30 days of a change in the Terrorism Threat Level?

8. Physical Security

_____ Does the Installation Commander coordinate and integrate subordinate unit physical security plans and measures into the AT plan?

_____ Are physical security measures considered, do they support, and are they referenced in the AT plan to ensure an integrated approach to terrorist threats?

Do AT physical security measures include provisions for the use of:

_____ Physical Structures.

_____ Physical Security Equipment.

_____ Chemical, Biological, Radiological detection & protection equipment.

_____ Security Procedures.

_____ Random Antiterrorism Measures (RAM)

_____ Response Forces

_____ Emergency measures sufficient to achieve the desired level of AT protection and preparedness to respond to terrorist attack.

_____ Are RAMs used for both in-place and transiting forces?

_____ Are special threat plans and physical security plans mutually supportive?

_____ Do security measures establish obstacles to terrorist activity (e.g., guards, host-nation forces, lighting, fencing)?

_____ Does the special threat plan include the threats identified in the threat statements of higher HQ?

_____ Does the physical security officer assist in the threat analysis and corrective action?

_____ Does the installation have and maintain detection systems and an appropriate assessment capability?

9. AT Guidance for Off-Installation Housing

_____ Are troops housed off-installation adequately secured?

_____ Do Sservice members in Moderate, Significant, and High threat areas receive instruction and supervision in residential security measures?

_____ In such areas, do unit AT response plans include current residence location information for all unit members residing off installation?

_____ In such areas, do units coordinate with local law enforcement authorities for protection of unit members residing off-installation (MOUs/MOAs/SOFs)?

_____ Do incident response plans include measures for off-installation personnel (personnel warning system)?

_____ Does the command have procedures to ensure DOD personnel assigned to Moderate, Significant, and High Terrorism Threat Level areas, who are not provided on-installation or other Government quarters, are furnished guidance on the selection of private residence to mitigate risk of terrorist attack?

_____ Does the command have procedures to conduct physical security reviews of off-installation residences for permanent- and temporary-duty DOD personnel in Significant or High Threat Level areas?

_____ Based on these physical security reviews, does the command have procedures to provide AT recommendations to residents and facility owners?

_____ As suitable, does the command have procedures to recommend to appropriate authorities the construction or lease of housing on an installation or safer area?

_____ Does the command have procedures to complete residential security reviews prior to personnel entering into formal contract negotiations for the lease or purchase of off-installation housing in Significant or High Threat areas?

_____ Does the command have procedures to include coverage of private residential housing in AT plans where private residential housing must be used in Moderate, Significant, or High Threat Level areas?

In Moderate, Significant, or High Threat areas, does the command incorporate family members and dependent vulnerabilities into antiterrorism assessment, mitigation, and reporting tools for:

_____ Facilities used by DOD employees and their dependents.

_____ Transportation services and routes used by DOD employees and their dependents.

_____ Has the staff judge advocate considered the ramifications of imposing these

housing policies in CONUS and advised on the consequences?

10. Security Structure

_____ Does the AT plan indicate that the FBI has primary domestic investigative and operational responsibility in the United States and US territories?

_____ Has coordination with the staff judge advocate been established?

_____ Does the plan allow for close cooperation among principal agents of the military, civilian, and host-nation communities and Federal agencies?

_____ Does the plan clearly indicate parameters for use of force, including the briefing of any elements augmenting military police assets?

_____ Is there a mutual understanding among all local agencies (e.g. military, local FBI resident or senior agent-in-charge, host-nation forces, and local law enforcement) that might be involved in a terrorist incident on the installation regarding authority, jurisdiction, and possible interaction?

_____ Has the staff judge advocate considered ramifications of closing the post (e.g., possible civilian union problems)?

_____ Does the AT plan identify DOS as having primary investigative and operational responsibility overseas?

11. Operations Center

_____ Has the operational command and coordination center (operations center) been established and exercised?

_____ Is the operational command and coordination center based on the needs of the installation while recognizing manpower limitations, resource availability, equipment, and command?

_____ Does the plan include a location for the operations center?

_____ Does the plan designate alternate locations for the operations center?

_____ Does the plan allow for the use of visual aids (chalkboards, maps with overlays, bulletin boards) to provide situation status reports and countermeasures?

_____ Does the plan create and designate a location for a media center?

_____ Have the operations and media centers been activated together within the last quarter?

_____ Does the operations center have standard operating procedures covering communications and reports to higher HQ?

_____ Does the operations center offer protection from terrorist attack?

12. Terrorist Incident Response Measures (first response)

Has the command prepared installation-wide and/or shipboard terrorist incident response measures which include:

_____ Procedures for determining the nature and scope of the terrorist incident and required response.

_____ Procedures for coordinating security, fire, and medical First Responders.

_____ Steps to reconstitute the installation's ability to perform AT measures

_____ In Moderate, Significant, or High terrorist threat level areas, has the command included residential location information for all DOD personnel and their dependents in their Incident Response Measures?

13. Rules of Engagement (ROE)/Rules of Force (RUF)

_____ Does unit have correct ROE/RUF guidance for the mission and environment?

_____ Do plan/current procedures provide enough "stand-off" to determine hostile intent and make proper decision to use force?

_____ Are troops trained for making ROE/RUF decisions in realistic situations?

_____ Are ROE/threat scenarios adequate & rigorous?

_____ Is unit prepared to apply ROE/RUF for threat scenarios?

14. Terrorist Consequence Management Measures

_____ Do CM measures provide for appropriate emergency response and disaster planning and/or preparedness to respond to a terrorist attack for the installation and/or base engineering, logistics, medical, mass casualty response, transportation, personnel administration, and local and/or host nation support?

_____ Do CM measures include guidelines for pre-deployment and garrison operations, pre-attack procedures, actions during attack, and post-attack actions?

15. General Observations

_____ Was the AT plan developed as a coordinated staff effort?

_____ Does the AT plan outline reporting requirements (e.g., logs, journals, after-action report)?

_____ Does the AT plan address presence of the media?

_____ Does the AT plan include communications procedures and communications nets?

_____ Does the AT plan consider the possible need for interpreters?

_____ Does the AT plan consider the need for a list of personnel with various backgrounds to provide cultural profiles on foreign subjects and victims, as well as to assist with any negotiation efforts?

_____ Does the AT plan provide for and identify units that will augment military police assets?

_____ Does the AT plan delineate specific tasking(s) for each member of the operations center?

_____ Does the AT plan provide for a response for each phase of antiterrorism activity (e.g., initial response, negotiation, assault)?

_____ Does the AT plan designate service support communications?

_____ Does the AT plan make provisions for notification of accident and incident control officer?

_____ Does the AT plan provide for EOD support?

_____ Does the AT plan take into consideration the movement from various locations, including commercial airports, of civilian and military advisory personnel with military transportation assets?

_____ Does the AT plan allow for the purchase and/or use of civilian vehicles, supplies, food, if needed (including use to satisfy a hostage demand)? Does the AT plan make provisions for paying civilian employees overtime if they are involved in a special threat situation?

_____ Does the AT plan take into consideration the messing, billeting, and transportation of civilian personnel?

_____ Do appropriate personnel have necessary language training?

_____ Is military working dog support available?

_____ Does the command review their own and subordinate AT programs and plans at least annually to facilitate AT program enhancement?

_____ Does the command review the AT ~~program~~ plan when the terrorist threat level changes?

_____ Has the command developed a prioritized list of AT factors for site selection for facilities, either currently occupied or under consideration for occupancy by DOD personnel? AT factors should include, but not limited to, screening from direct fire weapons, building separation, perimeter standoff, window treatments, protection of entrances and exits, parking lots and roadways, standoff zone delineation, security lighting, external storage areas, mechanical and utility systems.

_____ Has the command used these factors to determine if facilities can adequately protect occupants against terrorism attack?

APPENDIX F
FORCE PROTECTION CONDITION SYSTEM

1. General

a. Force Protection Conditions describe the progressive level of countermeasures in response to a terrorist threat to US military facilities and personnel as directed by DOD Directive 2000.12, *DoOD Antiterrorism (AT) Program*. These security measures are approved by the Joint Chiefs of Staff and are designed to facilitate inter-Service coordination and support of US Military antiterrorism activities. They are outlined in DODI O-2000.~~12-H~~16, *DoOD Antiterrorism Handbook*, Appendix 3, *DOD FPCON System*. When installations adapt these measures for their site-specific circumstances, they should account for, as a minimum, Combatant Commander/Service requirements, local laws, and SOFA. Per DOD Instruction 2000.16, *DoOD Antiterrorism Standards*, FPCON measures are FOR OFFICIAL USE ONLY. An AT Plan with a complete listing of site-specific AT measures, linked to an FPCON, shall be classified, as a minimum, CONFIDENTIAL. When separated from the AT Plan, specific measures and FPCON measures remain FOR OFFICIAL USE ONLY.

b. The FPCON System is the principal means through which a military commander or DOD civilian exercising equivalent authority applies an operational decision on how to best guard against the threat. These guidelines shall assist commanders in reducing the effect of terrorist and other security threats to DOD units and activities.

c. Creating additional duties and/or watches and heightening security enhance command's personnel awareness and alert posture. These measures display the command's resolve to prepare for and counter the terrorist threat. These actions shall convey to anyone observing the command's activities that it is prepared and an undesirable target, and that the terrorist(s) should look elsewhere for a vulnerable target.

d. The DOD system is generally not applicable to DOD elements for which the Chief of Mission has security responsibility, and may have limited application to DOD elements that are tenants on installations and facilities not controlled by US military commanders or DOD civilian exercising equivalent authority. Still, Commanders of US elements on non-US installations can execute many FPCON measures that do not involve installation level actions, at least to a limited degree. The terminology, definitions, and specific recommended security measures are designed to facilitate inter-Service coordination and support for the combating terrorism efforts of the DOD Components.

2. Force Protection Conditions

There are five FPCONs. Supporting measures for each condition are listed in Appendix 3 of DOD O-2000.12-H. The circumstances that apply and the purposes of each protective posture are as follows:

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

b. FPCON ALPHA applies when there is an increased general threat of possible terrorist activity against personnel or facilities, the nature and extent are unpredictable. ALPHA measures must be capable of being maintained indefinitely.

c. FPCON BRAVO applies when an increased or more predictable threat of terrorist activity exists. Sustaining BRAVO measures for a prolonged period may affect operational capability and relations with local authorities.

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

e. FPCON DELTA applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is imminent. Normally, this FPCON is declared as a localized condition. FPCON DELTA measures are not intended to be sustained for substantial periods.

3. FPCON Responsibilities

a. Geographic Combatant Commanders shall ensure that FPCONs are uniformly implemented and disseminated within their AOR.

(1) All military commanders and DOD civilians exercising equivalent authority are responsible for ensuring that their subordinates fully understand FPCON declaration procedures and FPCON measures.

(2) While there is no direct correlation between threat reporting and FPCONs, such information assists commanders in making prudent FPCON declarations. Existence of threat reporting in and of itself should not be the only factor used in determining FPCONs. FPCON declaration should be based on multiple factors that may include, but are not limited to, threat, target vulnerability, criticality of assets, security resource availability, operational and physiological impact, damage control, recovery procedures, international relations, and planned US Government actions that could trigger a terrorist response.

b. The ~~DOD~~ FPCON system allows all military commanders and DOD civilians exercising equivalent authority the flexibility and adaptability to develop and implement AT measures that are more stringent than those mandated by higher authorities whenever FPCONs are invoked. Each set of FPCON measures is the minimum that must be implemented when a change in local threat warrants a change in FPCON or when higher authority directs an increase in FPCON. Authorities directing implementation may

augment their FPCON by adding measures from higher FPCONs as necessary.

(1) Military commanders or DOD civilians exercising equivalent authority may implement additional FPCON measures from higher FPCONs on their own authority, develop additional measures specifically tailored for site-specific security concerns, or declare a higher FPCON for their AOR/installation.

(2) Subordinate military commanders or DOD civilians exercising equivalent authority at any level may not lower an FPCON or implement measures that are less rigorous than those appropriate for the declared FPCON. Waivers for not complying with prescribed FPCON measures may be obtained by following the procedures in paragraph 6 below.

(3) It is essential for military commanders and DOD civilians exercising equivalent authority to implement formal analytical processes that result in a set of ~~AOR~~ operational area or locality-specific terrorist threat indicators and warnings for use when transitioning from lower to higher FPCONs. Threat credibility, and if known, duration, operational environment (both HN and DOD), asset criticality, mission impact and measures in place that contribute to mitigating the current threat are but a few of the important elements commanders should consider when calibrating FPCON postures. Such processes and measures should be harmonized to the maximum degree possible, taking fully into account differences in threat, vulnerability, criticality, and risk of resources requiring protection.

(4) Military commanders, DOD civilians exercising equivalent authority, and their staffs shall examine the threat, physical security, terrorist attack consequences, and mission vulnerabilities in the context of specific DOD activities and the declared FPCON. When factors are combined and the collective terrorist threat exceeds the ability of the current physical security system (barriers, surveillance and detection systems, security forces, and dedicated response forces) to provide the level of asset protection required, then implementation of higher FPCONs or additional measures is appropriate.

4. FPCON Management and Implementation

Implementation of FPCONs does not come without adverse effects on day-to-day operations; the additional costs can be measured and described both quantitatively and qualitatively. The DOD FPCON system acknowledges cost as a significant factor bearing on the selection and maintenance of FPCONs. FPCONs ALPHA and BRAVO include measures that can be sustained for extended periods, consistent with the terrorist threat.

5. Random Antiterrorism Measures (RAMs) Management and Implementation

a. Commanders and Directors should randomly change their AT tactics; techniques, and procedures so that they ensure a robust security posture from which

terrorists cannot easily discern patterns or routines that are vulnerable to attack. An effective RAM program shall enable security to appear not only formidable but also unpredictable and ambiguous to instill uncertainty in terrorist planning. The basic approach for random antiterrorism measures program is to select security measures from higher FPCONs, as well as other measures not normally associated with FPCONs (command developed measures, or locally developed site-specific measures) that can be employed in a random manner to supplement the basic FPCON measures already in place. Using a variety of additional security measures in a normal security posture prevents overuse of security forces, as would be the case if a higher FPCON were to be maintained for an extended period of time. Selected RAMs offer an alternative to full implementation of a higher FPCON level. This is particularly important when terrorist threat estimates suggest that lower FPCONs may not, for the moment, be adequate in view of the risk, vulnerability, and criticality of DOD assets at the installation or facility.

b. To enhance the overall effectiveness of a given FPCON, unit commanders shall develop and implement a RAMs program as an integral part of their AT program. RAMs should be implemented in a strictly random manner, never using a set time frame or location for a given measure. RAMs should be visible (to confuse surveillance attempts) and should involve the command as a whole, not just the security forces. To be effective, tenant and transient units must be fully integrated into and support the installation or facility RAM program. Advantages of implementing RAMs include, but are not limited to:

(1) Enables commanders/directors to maintain/sustain a lower FPCON without compromising security effectiveness. Also, it maximizes scarce security resources and minimizes security force burnout and degradation in command AT awareness.

(2) Makes it more difficult, through variations in security routines, for terrorists to target important assets, build detailed descriptions of significant routines, or predict activities by a specific asset or within a targeted facility or installation. An Installation's tactical Deception Plan can be bolstered by the use of RAMS.

(3) Helps mask our capabilities to respond to, and defeat, terrorist attacks through unannounced, unpredictable, and visible security measures.

(4) Increases AT awareness for DOD personnel, their family members, visitors, and neighbors.

(5) Provides additional training and increases alertness of assigned security personnel and other participants through mental stimulation by changing their routine.

(6) Validates the installation or facility's capability to execute individual measures from higher FPCON.

(7) Provides a means to test the procedure, utilizing various methods, resources and personnel to ensure it can be effectively implement in an emergency.

(~~7~~8) Enables commanders/directors to more rapidly transition between FPCONs.

c. In summary, commanders/directors of defense agencies/facilities and their AT officers should keep the following tenets in mind when developing and executing their RAM program.

(1) The installation ATO is in charge of the RAM program, not the Provost Marshal or Security Officer if a separate entity/individual. However, the ATO should coordinate with the Provost Marshal/Security Officer regarding RAM measures that require utilization of security personnel. The ATO should monitor, track, and analyze RAM implementation efforts.

(2) A RAM program is part of a proactive and dynamic AT program.

(3) RAMs should include ~~be~~ visible actions in order to confuse surveillance attempts ~~(to confuse surveillance attempts)~~ and should involve the command as a whole, not just the security forces.

(4) To be effective, tenant and transient units must be fully integrated into and support the installation or facility RAM program.

(5) RAMs should be used throughout all FPCON levels and should include other measures not normally associated with an FPCON level such as Command developed measures, or locally developed site-specific measures.

(6) To confuse terrorist surveillance attempts, RAMs should be implemented in a strictly irregular fashion, never using a set time frame or location for a given measure.

(7) Local random antiterrorism measures should:

(a) Assess local threat capabilities and identify effective RAMs countermeasures.

(b) Mitigate installation/facility vulnerabilities.

(c) Be conducted both internally to the installation and externally in coordination with local authorities.

(d) Be compatible/coordinated with ongoing approved surveillance detection and security measures.

(e) Not be limited to security force personnel.

(f) Incorporate analysis of time and space considerations to allow security forces to maintain sufficient standoff while determining hostile intent.

d. A dynamic and proactive RAM program visibly communicates a command's resolve to prepare for and counter the terrorist threat. A RAMs program shall make it difficult for terrorist planners to discern security and defense and operational patterns. The terrorists should be compelled to look elsewhere for a more static, and therefore more vulnerable, target.

6. Deviations From Directed FPCONs

If it is determined that certain FPCON measures are inappropriate for current operations, or for proper threat mitigation, military commanders or DOD civilians exercising equivalent authority may request a waiver. The first general/flag officer exercising tactical control (TACON) for force protection or DOD civilian member of the senior executive service (SES) exercising equivalent authority in the chain of command is the approval authority for waiver of specific FPCON measures. Geographic combatant commanders, their deputies, or DOD civilians exercising equivalent authority, may delegate this authority below the general/flag officer level on a case-by-case basis. Any senior military commander having TACON for force protection or DOD civilian member of the SES exercising equivalent authority may withdraw first general/flag officer or DOD civilian authority and retain this authority, at his or her discretion. Waiver authority for specific FPCON measures directed by a higher echelon (above first general/flag officer or DOD civilian member of the SES) rests with the military commander or DOD civilian exercising equivalent authority directing their execution. Nothing in this waiver process is intended to diminish the authority or responsibility of military commanders or DOD civilians exercising equivalent authority, senior to the waiver authority, to exercise oversight of FPCON and RAMs program execution.

a. To ensure a consistent force protection posture is maintained, tenants on CONUS installations and facilities shall coordinate waiver actions with the host installation before submitting them to their chain of command.

b. All waiver requests shall be directed to the waiver authority. Information copies shall be sent to the combatant command's joint operations center, major/fleet command's operations center, service operations center, or DOD civilian operations center, as applicable.

c. Approved waivers, to include mitigating measures or actions, must be forwarded to Service, combatant command, major command, fleet, or DOD civilian equivalent command-level recipients within 24 hours.

7. Basic FPCON Procedures

a. Once an FPCON is declared, all listed security measures are implemented immediately unless waived by competent authority as described above. The declared FPCON should also be supplemented by a system of RAMs in order to complicate a terrorist group's operational planning and targeting. Specific measures for each FPCON are listed in Appendix X.

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

(2) Due to their specific security requirements, DOD ships' measures are listed separately. Those measures applying solely to US Navy combatant ships are further identified. Shipboard guidelines are specially tailored to assist commanding officers and ship masters in reducing the effect of terrorist and other security threats to DOD combatant and non-combatant vessels, to include US Army and Military Sealift Command ships worldwide. They provide direction to maximize security for the ship based on current threat conditions consistent with performance of assigned missions and routine functions.

b. Specific countermeasures were determined taking into consideration the following factors:

(1) Ability to maintain highest state of operational readiness.

(2) Measures to improve physical security through the use of duty and guard force personnel limit access to the exposed perimeter areas and interior of the unit/facility by hostile persons, and barriers to physically protect the unit/facility.

(3) Availability of effective command, control, and communication systems with emphasis on supporting duty/watch officers, security forces, and key personnel.

(4) An AT awareness program for all personnel.

(5) Protection of high-risk assets and personnel.

(6) Measures necessary to limit activities, and visitor/social engagements.

c. FPCON NORMAL and all FPCON levels should include site specific measures a facility commander deems necessary when establishing a baseline posture.

Intentionally Blank

APPENDIX G
MARITIME SECURITY CONDITIONS

1. General

a. The Coast Guard's Maritime Security (MARSEC) Conditions allow security measures to be escalated as the threat increases. Very similar to the 5 colors used by the ~~Office~~ Department of Homeland security to set domestic security levels, MARSEC conditions help to ensure that the security measures in place are appropriate for the threat level, given the multiple uses of the maritime sector.

b. Each incremental increase in security is valuable; whether it is designed to detect, deter, or defend against an attack. A comprehensive security plan must include strategies that cover this entire spectrum.

c. The level of security appropriate for a given target is dependent on all three axes of the risk equation: consequence, vulnerability, and threat, and must be able to detect, deter, or defend on those axes.

d. For each MARSEC level determine:

(1) Access control.

(2) Restricted areas.

(3) Handling of cargo.

(4) Delivery of stores / supplies.

(5) Security monitoring.

(6) Security duties.

2. MARSEC I.

a. MARSEC I is the "new normal". It represents the baseline threat we live with everyday - heightened security and balance in all missions with stronger interagency coordination. Security measures in MARSEC I are the minimum measures which should be sustainable indefinitely.

(1) Focuses on increased awareness and associated increases in assets dedicated to port security missions.

(2) Establishes command and control (C2) and intelligence foundation for heightened levels of maritime security.

(3) Requires significant resources to establish new programs (Sea

Marshals, Port Vulnerability Assessment & Intelligence/Investigation teams) in all ports and to bolster US Coast Guard and other government agency (OGA) assets in selected high priority ports.

(4) MARSEC I is generally equivalent to Homeland Security Advisory System (HSAS) conditions Green, Blue, and Yellow.

b. Activities:

(1) Increased intelligence & fusion.

(2) Increased visibility of cargo, people, & vessels.

(3) Enhanced C2 interoperability/ connectivity.

(4) Increased Security Zones.

(5) Increased port security patrols.

(6)Increased control of vessel movements.

(7) Increased protection of assets & critical infrastructure.

(8) Increased air surveillance in port and offshore.

(9) Enhanced risk management – high interest vessels.

(10) Improve Federal / State / local / private sector coordination / intelligence / information sharing.

(11) Research and development.

(12) Require / approve / exercise security plans (facility/vessel port).

(13) Increase facility / vessel security inspections.

c. Capabilities:

(1) Intelligence & Investigation Teams.

(2) Port Vulnerability Assessment Teams

(3) Advanced Notice of Arrival.

(4) Vessel / Facility / Port Inspection Teams.

(5) Improved C2 systems.

(6) Increased boats/crews in strategic ports.

(7) Increased aircraft flight hours.

(8) Vessel Traffic Systems / automated identification system.

(9) Increase port security surge capability.

(10) Sea Marshal Teams.

(11) Maritime Safety and Security Teams.

(12) Pollution Strike Teams.

(13) Contingency planners.

(14) Other Federal, State & local agencies.

(15) Private sector.

3. MARSEC II.

a. MARSEC II is set when there is a heightened threat of an unlawful act against a port, facility, vessel, or other component of the marine transportation system and intelligence indicates that terrorists are likely to be active within a specific period or a specific area, or against a specific class of target. The risk level may also indicate that a specific segment of the industry may be in jeopardy but no specific target is identified. Security measures in MARSEC II should be sustainable for as long as the threat lasts.

(1) Heightened Risk – Focused Security, Prioritized Missions.

(2) MARSEC II corresponds to HSAS level Orange.

b. Activities: All MARSEC I activities plus:

(1) Movement of major cutters and patrol boats to selected ports.

(2) Heightened port control & security.

(3) Increased air surveillance of port and its offshore approaches.

(4) Increased critical infrastructure protection.

(5) Increased Aids to Navigation and ice breaking services as required.

c. Capabilities: All MARSEC I assets plus:

(1) Limited Reserve Component call-up.

(2) Deploy Maritime Safety and Security Teams.

(3) Increased level of small boat & cutter resources.

(4) Increased aircraft flight hours.

(5) Enhanced DOD & OGA support.

(6) Enhanced posture will be result of limited reserve call-up, targeted redirection of USCG assets to port security missions, and increased reliance on DOD/OGA support.

(7) Other CG mission performance will degrade without significant increase in resources (Cutters, boats, aircraft, personnel)

4. MARSEC III.

a. MARSEC III is set when an attack is thought to be imminent or intelligence indicates that terrorists have chosen specific targets, or an attack has already taken place and there is indication that similar targets or other targets in the same region may be at jeopardy. MARSEC III measures should be sustainable for about 7 days.

(1) Incident Imminent – Exert Control, Stop Doing Other Missions.

(2) MARSEC III corresponds to HSAS level Red.

b. Activities: All MARSEC II activities plus:

(1) Specific movement of major cutters and patrol boats to high risk ports.

(2) Highest level of port control & security.

(3) Highest level of air and surface surveillance of port and its offshore approaches.

(4) Highest level of protection for critical infrastructure.

(5) Increased Aids to Navigation and ice breaking services as required.

c. Capabilities: All MARSEC II assets plus:

(1) Partial mobilization of Reserve component.

(2) Additional small boats, cutters, & crews.

(3) Additional fixed/rotary wing aircraft & crews.

(4) Increased DOD & OGA support.

(5) Enhanced posture will be result of partial reserve mobilization, redirection of all CG assets to port security missions, and heavy reliance on DOD/OGA support.

(6) Posture will only be sustainable for very short period of time (2-3 weeks).

5. Considerations

a. **Security vs. access**.

(1) Security measures may restrict use of waterways.

(2) Security measures may restrict access to information.

b. **Security vs. commerce**. Almost every security measure implemented serves to impede commerce, either indirectly by delaying ships and cargo, or by adding direct cost.

c. **Security vs. environment**. Not only are resources potentially shifted from environmental protection and response missions to security missions, but some of the increased security measures come at the expense of the environment. These include:

(1) Security initiatives may take resources away from pollution prevention and response.

(2) Security measures may require more land and water be available for commercial use.

(3) Limited access (physical and cyber) may adversely impact response effectiveness.

(4) Hampering effective environmental response due to restrictions on physical and cyber access.

d. **Security vs. safety**. Security measures should be crafted in a way that does not jeopardize safety.

(1) Increased duties related to security may cause crew fatigue or may divert attention from vital safety functions.

(2) Access controls limit resources on hand to prevent incidents.

APPENDIX H
HIGH RISK PERSONNEL PROTECTION

1. General

a. The combatant commanders have substantial AT responsibility for DOD personnel in their AORs assigned to high-risk billets (HRB) or high-risk positions. High risk personnel (HRP) assigned to high-risk positions become eligible for advanced AT training and protection.

b. The designation of personnel or billets as "high-risk" imposes a requirement on both the incumbents and the government to take special precautions to ensure the safety and security of these individuals and their family members.

2. High Risk Personnel Protection

a. DOD Directive 2000.12, *DoDD Antiterrorism (AT) Program*, addresses the need to provide protection to those military officers, DOD civilians, and their family members who are assigned to high risk billets and/or by virtue of their rank or grade, assignment or symbolic value, or relative isolation, are more likely to be attractive targets to terrorists.

b. DOD Instruction 2000.16, *DoDD Antiterrorism Standards*, establishes two standards directly pertaining to "Training for High Risk Personnel and High Risk Billets" and "Executive Protection and High Risk Personnel Security". Chapter 18 of DOD O-2000.12-H, *DoDD Antiterrorism Handbook*, provides specific information on the training programs available for DOD executives.

c. Protective Service Operations (PSO) entail the protection of dignitaries and other high risk personnel in the combatant commander's area of responsibility where significant threat exists. Those threats include assaults, kidnappings, assassinations, and attempts to embarrass the US Government. For purposes of this appendix, the term "executive" applies to all persons requiring additional security protection because they are assigned to high risk billets or have been designated as high risk personnel.

d. The specific supplemental security measures that may be furnished to executives are subject to a wide range of legal and policy constraints. US law establishes stringent requirements that must be met before certain security measures may be implemented. DOD component regulations, instructions, and legal opinions may further constrain implementation of the executive protective measures described in this appendix. SOFAs and MOUs between the US Government and a foreign government shall also limit use of supplemental security measures. The US Government contracted use of land or buildings for use by the Department of Defense may also limit application of certain security techniques. All of these constraints should be carefully considered when conducting security surveys, developing plans, and implementing additional security measures to protect executives.

3. Executive Protection Goals

a. In the discussion that follows, several measures are outlined which can afford DOD executives additional protection against terrorist acts. The primary purpose underlying these measures is to:

(1) Delay at a Distance. Increase the time that elapses between the detection of an imminent terrorist attack and the actual onset of an attack to permit the arrival of response forces or the successful evacuation of executives.

(2) Delay to Permit Flight. Increase the amount of time that elapses between the onset of an attack and terrorist access to executives to permit the arrival of response forces or the successful evacuation of executives under attack.

(3) Delay, Hold, and Counterattack. Increase the duration of an attack by allowing executives, their staffs, and their families to remain secure in a safe haven until a response force can arrive to repulse the attack, apprehend the terrorists, and relieve the executives and those with them in the safe haven.

b. Each supplemental security measure should be applied judiciously. There is a clear trade-off between increasing the level of executive office and residence AT measures and the need to preserve the anonymity of executives to avoid activity that may point to the executive's prominence or criticality.

c. Supplemental AT measures can be expensive. The expense should be measured not just in terms of dollars, but also in terms of changes to organizational routine. Therefore, two primary questions must be addressed prior to the implementation of potentially bold, disruptive, and expensive supplemental security enhancements.

(1) What are the most cost-effective means of enhancing the security of executives at risk? How many changes in organizational routines and personal behavior shall have to be made in order for security measures to be effective in reducing the vulnerability of executives and the risk of terrorist attacks?

(2) What are the anticipated costs of additional security measures in terms of dollars, organizational functionality, and mission capability?

d. The security enhancements described in this appendix shall be even more effective if the executives and their families take full advantage of the enhancements and reinforce the security measures. If executives do not change their behavior to accommodate additional security and protective measures, then their behavior can effectively defeat the purpose of the additional protection.

e. Security measures can be enhanced to deter almost any terrorist threat. However, there may be a point where it is no longer economical to add layer upon layer of protective measures to deter a threat that is capable of overwhelming available

protective measures. When facing a well-armed and capable terrorist threat, additional security measures coupled with an alternative security posture may provide the greatest deterrence to a terrorist attack.

4. Supplemental Security Measures for Executives.

Sound AT principles apply to both executive offices and residences. The following principles should be reviewed prior to implementing supplemental AT measures.

a. A thorough physical security survey serves as the foundation for a strong executive protection program. Physical security surveys of the offices and residences of DOD elements and personnel attached to US Embassies should be performed by the DoS. Cognizant physical security and facilities engineering staffs should perform surveys of other DOD facilities.

b. The optimal approach to a physical security site survey is from the viewpoint of a potential terrorist. The survey should examine avenues of approach to the installation, facility, or residence; points of access to the executive offices or residences; and how attacks on offices, residences, or other frequently used facilities could be mounted.

c. A technical threat assessment is the next step in evaluating the need for supplemental executive AT measures. It provides a thorough and detailed assessment of the weapons and tactics terrorists might use to attack the structure where DOD executives work and reside, as well as providing the basis for the development engineering design requirements. (See DOD O-12000.12-H, Chapter 21, *Individual Protective Measures*, for detailed information on a thorough technical TA.).

d. A technical assessment of responses provides engineers information on the anticipated performance of the security forces responding to a terrorist threat and the expected or desired behavior of the protected executives.

e. Security planners require information on the expected duration of a terrorist attack on the structure housing executives prior to security force response. A comparison of terrorist threat capabilities and the security response force capabilities provides significant AT system performance parameters. These parameters can be quantified and used to develop detailed plans, drawings, and AT equipment acquisition plans.

f. While AT enhancement measures are intended to provide additional protection for executives, the primary purpose of these measures is to increase time required by terrorists to penetrate the executive's office or residence.

5. Security in the Office

a. The office environment should normally provide executives the greatest

degree of AT protection. AT measures, guards, security checkpoints, office workers, aides, and/or secretaries all serve to insulate the executives from potential threats. Unfortunately, the considerable media attention provided to attacks on executives in government facilities may further entice terrorists. Hence, there may be a need to enhance security measures to offset the escalating capability of attack on more secure office areas by terrorist groups.

b. The following measures can be selectively implemented to enhance executive office AT security:

(1) Increase Threat Detection Time by installing sensors on perimeters and barriers.

(a) Install surveillance systems, including seismic, acoustic, and infrared sensors at or beyond the outer perimeter; supplement these systems with closed circuit TV and/or imaging infrared systems tied into the alert security response force staging area.

(b) Extend restricted areas or exclusion zones and relocate access control points from the executive's office or residence to a point closer to the boundary of the installation.

(c) Increase and extend intrusion detection sensors from within the installation or facility perimeter to the installation perimeter, allowing the sensors to collect additional data in order to classify and identify an intrusion before the response force arrives at scene or track of the intruder.

(d) Increase the number of surveillance and duress detection systems within the executive office area as well as approaches to the office area.

(2) Increase Threat Delay Time between perimeter and executive office building.

(a) Install vehicle barriers and realign roadways to eliminate straight, level stretches of road in excess of 50 meters in length.

(b) Increase concentric rings of fences, Jersey barricades, planters, bollards, and vehicle and/or personnel barriers.

(c) Install access control areas, supplemented by fire doors and/or security doors kept in a closed condition, between the entrance to the building housing executive offices and the executive office area itself.

(d) Confuse, Camouflage, and Deceive Observers by Hiding Executives' Locations.

(e) Consider relocating executives to buildings not usually associated with office activities, e.g., barracks, motor pool, R&D facilities.

(f) Consider constructing office areas in barracks, motor pool, R&D facilities, etc.

(g) Add executive style, decorative lighting and window treatments to several different areas of office buildings to minimize differences in external appearances between executive and non-executive offices.

(3) Increase Delay Time between the entrance to the building housing executives and the executive office area.

(a) Consider the addition of fire doors, access control points, dead-end corridors, and mid-corridor physical barriers to complicate access to executive office areas.

(b) Consider the addition of security devices which when activated disrupt the ability of intruders to retain their thought processes. These types of security devices include flashing strobe lights, fog generators, noise generators, sirens, and fire extinguishing systems.

(4) Increase Delay Time and make access more difficult within the executive office structure.

(a) Replace standard doors and doorframes in areas leading to executive offices with high security doors and doorframes.

(b) Install high security grating; wire mesh, or other materials to bar access to executive's office area through utility tunnels or conduits.

(c) Strengthen walls, floors, and ceilings against improvised explosive devices, small arms fire, incendiary devices, and powered hand tools by substituting steel plate, concrete filled, steel reinforced cinder blocks, or other ballistic resistant materials for plaster/lath or wallboard room dividers.

(d) Add steel plates or other ballistic materials in crawl spaces above dropped ceilings; extend walls separating executive office area from other portions of an office building to prevent unobserved and undetected access to space of dropped ceilings.

(5) Increase hold time to contain penetrators.

(a) Add positive action controls to facility and doors and gates to ensure the gates and doors default to a closed and locked condition unless manually released.

(b) Add positive action controls to access control areas such that persons inside an access control area can neither advance nor withdraw without affirmative action by a security officer posted outside the access control area.

(6) Increase protection for building occupants against ballistic threats to windows and exterior walls.

(a) Substitute polycarbonate panels for glass windows; add a ballistic absorbing plastic film to the interior side of glass windows.

(b) Add exterior screens/plates to cover window areas and protect against gunfire and grenade/bomb fragments.

(c) Install blast curtains, metal blinds, metal shutters or other window treatments in executives' offices to protect interior space from glass shards and other small projectiles.

(7) Install emergency executive support facilities including a safe haven with duress system and telephone, and an emergency evacuation capability.

(a) Consider installation of helicopter landing aids on the roof of a structure or on an adjacent field far removed from parking areas.

(b) Consider installing a safe haven or other reinforced security structure adjacent to a helicopter landing facility to provide a secure waiting place for executives until a rescue helicopter with additional supporting air and ground units can extract the executives.

(8) Office Security Practices and Procedures.

(a) Executives should discourage their staff from disclosing the executive's whereabouts or activities when taking telephone messages.

(b) An executive's staff should use caution when opening executive mail. In particular, the staff should look for letters or packages that might contain improvised explosive devices, or evidence of biological agents, e.g., suspicious white powder.

(c) Strictly limit access to the executive office area.

(d) Limit publicity about the executive to a bare minimum; keep official biographies short; provide minimal information concerning the executive's personal interests and hobbies, and consider using outdated photographs if a publicity photograph is absolutely essential.

(e) The executive should avoid working alone, late at night, and on days when the remainder of the staff is absent.

(f) If late night work is necessary, the executive should work in conference rooms or internal offices where observation from the outside of the building is not possible. The executive should notify the security force that they shall be working late and ask that they look in periodically. Executives should enter and exit several offices, turning lights on and off before going to their own offices to disguise the purpose of their activities to outside observers.

(g) Executives should avoid placing office furnishings directly in front of exterior windows.

(9) Official business away from the office.

(a) Executives and their staff should discuss security requirements with the person planning the function.

(b) The executive should travel to and from the function with an escort.

(c) The executive's travel route should be chosen carefully to avoid potential hazard areas.

(d) The executive's planned attendance at official functions should not be publicized if at all possible.

(e) An attempt should be made for the executive to sit away from both public areas and windows.

(f) The sponsor(s) of the function should be encouraged to close the curtains to minimize the likelihood that anyone outside shall be able to see inside and determine who is attending the function and where they are located. This is extremely important for an evening function, when a well-lit interior can be easily viewed from a darkened exterior.

(g) The executive's staff should request that external floodlights be used to illuminate the area around the building where an evening function shall occur.

6. Residential Safety

The residential environment may provide executives a more limited degree of AT security. Executive residences are often located in more secluded areas of the installation or off the installation in the local economy and therefore may appear to present a "softer target" to terrorists. AT measures, guards, security checkpoints,

household staff, aides, and/or secretaries can assist in insulating the executives from potential threats. An executive's entire lifestyle should be included in security surveys used to assess the need for supplemental AT security measures. The executive's residence and transportation between the residence and the office should also be examined for vulnerabilities.

a. The same principles used to identify supplemental AT improvements in an office environment apply to executives' home environments as well. Recall that the purposes of AT enhancements are:

(1) Increase the amount of time terrorists need to initiate and complete an attack on executives while at home, thereby giving response forces more time to rescue executives and their family members.

(2) Reduce the potential threat to executives and their families as a consequence of a terrorist assault mounted against the residence.

(3) Increase the amount of time between detection of a threat and the onset of hostile actions.

(4) Delay the terrorists as long as possible; prevent their access to the executives and their family members on the one hand, and make the terrorists' departure from the scene to escape prosecution difficult; provided that in so doing, the lives of executives and their family members are not further jeopardized.

(5) Provide a safe haven that executives and their family members may flee for security pending the arrival of a security response force.

b. Site Selection.

(1) Avoid selecting residences previously used by other senior US Government or foreign government officials.

(2) Avoid selecting residences previously attacked by terrorist groups.

(3) While terrorist groups conduct surveillance to identify targets, mistakes have been made in the past. DOD personnel should avoid leasing residences previously used by representatives of governments or organizations known to be targets of various terrorist groups. DOD personnel leasing residences formerly used by representatives of such governments may be placing themselves unnecessarily at risk of being attacked as a result of mistaken identity.

c. The following measures can be selectively implemented to enhance executive residential security:

(1) Increase time interval between detection of a threat and the onset of

hostile terrorist acts.

(a) Ensure all door locks and window clasps are working.

(b) Ensure that all doors and windows are properly secured to their frames and the frames are properly anchored to the residential structure.

(c) Consider locking the driveway gates with a security lock to deter/delay entry.

(d) Consider installing a through-door viewing device or visitor intercom.

(e) Consider installing security lights to aid in viewing entrances.

(f) Increase the number of physical barriers between the outer perimeter of the residence and the interior of the residence.

(g) Add heavy, remotely operated gates to all fences, walls, and perimeter barriers, consistent with the penetration resistance of the barrier, between the residence, the street, and adjacent neighbors.

(h) Create a vestibule or "air lock" between living quarters and the exterior of a residence to ensure that no one can go from outside the residence directly into the residence.

(i) Add fire doors or security doors/gates between the bedroom areas and living areas of the residence.

(2) Increase the time required to penetrate exterior structural walls with explosives, hand-held power tools, and hand tools.

(a) Consider the addition of additional armor covered by aesthetically pleasing materials to exterior walls.

(b) Consider the addition of a separate reinforced masonry wall around the residence.

(3) Increase surveillance of residence and decrease response time.

(a) Consider installing closed circuit TV systems to permit remote viewing of all residential doors and windows accessible from the ground, nearby structures, trees, or easily acquired platforms (e.g., van parked next to a wall).

(b) Consider installing area intrusion detection systems

between the residence perimeter and the residence itself. Increase the number and types of sensors. Add backup communication channels between the intrusion detection system and a surveillance assessment and/or response dispatch center.

(4) Increase the durability and survivability of the residence to terrorist attack.

(a) Consider fitting windows with either Venetian blinds or thick curtains to reduce the visibility of activities within the residence and to reduce hazards of flying glass in the event of nearby explosions or gunfire.

(b) Install backup power systems for security devices, to include: surveillance systems, communication systems, and access control systems.

(c) Establish backup communications with the installation or embassy security department via secure landline or two-way radio.

(d) Consider placing a panic alarm bell to the outside of the house with switches on all floors of the residence. The panic alarm should also annunciate at the local police and the appropriate DOD or DOS security office.

(e) Install a safe haven in the home.

(5) Home Security Practices and Procedures.

(a) Executives, family members and staff should check persons entering their residences; e.g., electricians, plumbers, telephone maintenance personnel. If in doubt, the executive should call the person's office to verify the person's identity before allowing them into the residence.

(b) Executives should not open the door to a caller at night until the caller is identified by examination through a window or door viewer.

(c) The curtains in an executive's residence should be closed before turning on lights.

(d) Executives should consider placing the telephone where the executives shall not be seen from doors or windows when answering.

(e) Executives should investigate household staff (especially temporary staff).

(f) Executive should always be on the lookout for unusual activities and ensure their residence is locked and secure whenever the residence is unattended. Executives should be cautious upon returning to their residence.

(g) Executives should note and report suspicious persons.

(h) Executives should strictly control house keys.

(i) Executives should secure their vehicles in locked garages.

(j) Executives should be alert for the unusual, such as the movement of household furniture or the identification of unusual wires.

(k) The executive should consider the installation of a panic alarm bell on the exterior of the residence, with the placement of annunciator switches on every level of the residence.

(l) The area surrounding the executive's residence should be cleared of dense foliage or shrubbery.

(m) If the executive's residence is equipped with a duress alarm, the alarm should be routinely tested. Members of the executive's family should understand how the duress alarm works and the situations when the alarm should be activated.

(n) Executives should cooperate with ~~law enforcement~~ security personnel and abide by their ~~security~~ recommendations concerning ~~your~~ home~~'s~~ security.

7. Security at Social and Recreational Activities.

Executives shall routinely be at risk to terrorist incidents, but they must continue with their professional as well as personal lives. The following measures are intended to permit executives to continue living as close to a normal life as possible while still remaining mindful of the risks to their security.

a. Executives should ensure their hosts are aware of the executive's need for security and that the host establishes appropriate security measures.

b. Executives should have their personal staff assist a civilian host if required.

c. Executives should arrange for visitors to be subject to adequate security control.

d. Executives or their staff should screen the invitation lists, if possible.

e. Executives should vary the times of their athletic activities, such as golfing, jogging, etc.

8. Travel Safety

a. Executives are most often at their peak accessibility to terrorists when they are in transit in official or privately owned vehicles. This section recommends steps to reduce the vulnerability of executives while in transit. Implementation of measures to enhance the transportation security of DOD executives must be in full compliance with US laws and DOD directives.

b. The domicile to duty transportation policy follows:

(1) As a general rule, Congress has strongly opposed provision of home to office (domicile to duty) transportation by the Federal Government to its officers and employees. Congress did, however, grant authority to the President and the heads of executive agencies and departments to provide domicile to duty transportation under certain circumstances. According to statute, "a passenger carrier may be used to transport between residence and place of employment. An officer or employee with regard to whom the head of a Federal agency can make a determination, [if] that highly unusual circumstances present a clear and present danger, that an emergency exists, or that compelling operational considerations make such transportation essential to the conduct of official business."

(2) The phrase, “highly unusual circumstances which present a clear and present danger”, is understood to mean that the perceived danger is:

(a) Real danger, not imagined.

(b) Immediate or imminent danger, not merely potential danger.

(c) A showing is made that the use of a government vehicle would provide protection against the danger that would otherwise not be available.

(3) The phrase, “emergency exists”, is understood to mean that there is an immediate, unforeseeable, temporary need to provide home-to-work transportation for an agency's essential employees.

(4) The phrase, “similarly compelling operational considerations,” is understood to mean that there is an element of gravity or importance to the need for government furnished transportation "comparable to the gravity or importance associated with a clear and present danger or an emergency situation." The Congress suggested further, "in such instances, [it is expected] that home-to-work transportation would be provided only for those employees who are essential to the operation of the Government.

c. Local official and unofficial travels.

(1) Executives should vary their daily pattern as much as possible, leaving and returning to their office or residence at different times.

(2) Executives should consider escorts to and from work, or travel with a neighbor.

(3) Executives should establish a simple duress procedure with their drivers. Any oral or visual signal shall suffice (i.e., something that the executive or driver says or does only if something is amiss).

(4) When using a taxi service, the executive should vary the taxi company. The executive should ensure that the identification photo on the taxi license matches the driver. If the executive is uneasy for any reason, the executive should simply take another taxi.

(5) When attending social functions, executives should attend the event with other guests if possible.

(6) Executives should examine their vehicle before entering to see if there has been any interference. A small mirror on a rod is a cheap and effective method to inspect underneath cars. Executives should not touch their vehicles until it has been thoroughly checked (look inside it, walk around it, and look under it).

(7) Executives should not leave personal items exposed in their vehicle, e.g., uniform items, service issued maps, official briefcases, etc.

(8) Executives should use the same precautions when driving their privately owned vehicle (POV) or a government owned vehicle (GOV).

(9) Executives should keep their car doors locked and not open windows more than a few inches.

(10) Executives should never overload a vehicle and ensure that all persons wear seat belts.

(11) Executives should always park vehicles in parking areas that are either locked or watched and never park overnight on the street. Before entering vehicles, executives should check for signs of tampering.

(12) Executives should keep the trunk of their vehicle locked.

(13) Where feasible, executives should drive in the inner lanes to keep from being forced to the curb.

(14) Executives should use defensive and evasive driving techniques. Executives should drill with their drivers by watching for suspicious cars and taking evasive action.

(15) Executives should avoid driving close behind other vehicles, especially service trucks, and be aware of activities and road conditions two to three blocks ahead.

(16) Executives should be aware of minor accidents that could block traffic in suspect areas. Crossroads are especially dangerous because they are preferred areas for terrorist or criminal activities since crossroads offer escape advantages to the attacker.

(17) Executives should take the following actions if they are attacked and a roadblock is encountered:

(a) Use the shoulder or curb (hit at a 30- to 45-degree angle) to go around the roadblock.

(b) If needed, ram the terrorist blocking vehicle in a non-engine area, at a 45-degree angle, in low gear, and at a constant moderate speed. The main purpose of ramming the vehicle is to knock the blocking vehicle out of the way. In all cases, the executive's vehicle should not stop and the executive's vehicle should never be boxed in with a loss of maneuverability. Whenever an executive's vehicle veers away from a terrorist vehicle, the executive's vehicle is placed in an adverse position and it presents a better target to gunfire.

d. Interurban, national, and international travel security practices and procedures.

(1) Executive airline seats should be booked at the last moment. If possible, the executive's seats should be booked using an alias.

(2) The use of an executive's rank or title should be restricted.

(3) Executives should not allow unknown visitors into their hotel room or suite.

(4) Executives should keep their staff and family members advised of their itinerary and subsequent changes to the itinerary. Executives should strictly restrict their itinerary information to only those individuals who require this information as a part of their official duties.

e. Statutory Authorities and Limitations.

The Secretary of Defense has statutory authority to allow a combatant commander to use government owned or leased vehicles to provide transportation in an area outside the United States for members of the uniformed services and other DOD personnel under certain circumstances. Such circumstances include and are limited to a determination by the combatant commander that public or private transportation in the

area is unsafe or is not available. Under such circumstances, the Department of Defense may provide transportation, usually in government buses or passenger vans to personnel and their family members if in so doing, it shall permit the combatant commander and his subordinate commanders to maintain capability to perform or to undertake assigned missions. Such transportation is not intended to be used to convey persons from their residences to their places of work.

f. DOD Non-tactical Armored Vehicle Policy.

(1) It is DOD policy to make non-tactical armored vehicles (NTAV) available where necessary to enhance the security of high-risk personnel, consistent with the requirements and limitations found in DOD Directive C-4500.51, *DoOD Non-Tactical Armored Vehicle Policy*. DOD issuances, Service regulations, and combatant commander guidance stipulate detailed procedures through which the Department of Defense manages NTAV programs.

(2) The Department of Defense categorizes non-tactical armored vehicles as heavy non-tactical armored vehicles (HAV) and light non-tactical armored vehicles (LAV) (these are normally armored sedans or sport utility vehicles).

(a) HAVs are fully armored vehicles intended to protect occupants from terrorist attacks using bombs, improvised explosive devices, grenades, and high velocity small arms projectiles. These vehicles are authorized on a case by case basis for designated high-risk personnel by ASD (SO/LIC). Factors to be considered are:

1. Country Threat Level. HAVs are for use primarily overseas in countries with High Terrorist Threat Levels. Considerations include the threat capability and vulnerability of the target, and environment in which the threat operates.

2. Protection Level. The threat must warrant the increased protection an HAV provides.

3. Availability of Existing Assets. Diversion of existing HAVs is not possible.

(b) LAVs are less than fully armored vehicles (normally armored after purchase) intended to protect occupants from terrorist attacks using medium velocity small arms projectiles and at least some types of improvised explosive devices. LAVs are used to protect high-risk personnel who require protection but are not authorized the use of an HAV.

(3) Each of the Departments and some Defense Agencies (DIA, NSA, etc.) manage a portion of the DOD Non-Tactical Heavy Armored Vehicle Program. Each of these components has issued supplementary mandatory guidance on processing of requests for, as well as allocation and use of, these scarce assets.

(4) HAVs are complex systems requiring specialized maintenance and operation. As a general rule, HAVs shall be assigned to DOD personnel with a driver who has been properly trained in the operation and maintenance of the vehicle. The operator is not a chauffeur; he or she is an integral part of a supplemental security package provided by the Department of Defense to meet its obligations to protect its key assets. HAVs are only justified where highly unusual circumstances present a clear and present danger to the health and safety of a nominated protectee, or compelling operational considerations make such transportation essential for the conduct of official business.

(5) LAVs may also be provided by the US Government to DOD executives where "highly unusual circumstances present a clear and present danger to the health and safety of a nominated protectee or compelling operational considerations" warrant their use. This category of non-tactical armored vehicle features "add-on" or "kit" armoring. While a less complex armoring system than those used in heavy NTAVs, "light" NTAVs afford substantial protection to occupants against a wide variety of threats. New developments in after manufacture armoring kits for vehicles are occurring at a rapid pace, increasing the number of vehicle manufacturers and models for which "other NTAV" modifications are suitable.

(6) The use of privately owned vehicles by high risk personnel is not recommended during periods of high risk. Armored non-tactical vehicles shall be used when available. High risk personnel and their protective details should take the appropriate measures identified in appendixes 12 and 13 of DOD O-2000.12-H

9. Protective Security Operations

a. Each Department is authorized to provide Protective Security Details (PSD) for key senior military officers, DOD civilians, other US Government officials or foreign dignitaries requiring personal protection.

b. Each Department's Secretary upon recommendations of their counterintelligence and/or law enforcement investigation staffs makes assignment of PSDs to executives. PSDs are assigned to DOD personnel who meet requirements established by Service regulations. In general, PSDs may be assigned only to those executives whose position or assignment places them at risk and whose continued availability to the President, Secretary of Defense, and combatant commanders is vital to the execution of DOD missions.

c. General Security Concept. Protective Security Details provide high levels of security to an executive (protectee) by establishing a series of protective cordons around the executive. The establishment of defense in depth often means that the innermost protective layer is in close contact with the protectee at all hours of the day and night.

d. Maintenance of Low Profiles. PSDs are trained in the art of maintaining low

profiles. Not only are they concerned about the visibility of the protectee, they are also concerned about their ability to blend the protectees into the surrounding environment. The security of a protectee is severely damaged when the presence of the PSD is obvious and detectable, when all other measures to blend the protectee into the local environment have been successful.

e. PSDs shall strive to limit the publication of the protectee's travel routes and means of transportation. If the protectee's travel routes and means of travel must be published, the PSD may suggest editorial changes to the itinerary scheduled for public release in order to limit details of the protectee's travel. For example, routes to and from announced appointments usually do not need to be released to the public.

f. PSD Mission Duties.

(1) During the course of a PSD mission, members of the PSD may be asked to perform several different security functions. They may, for example, perform direct or indirect protection or escort duties. Direct protection is open and obvious; indirect protection is generally a surveillance measure. The security guard unit may operate as an interior guard and may consist of one or more PSD members stationed at fixed posts. PSD members should know the identity of each individual in the protectee's party; protectees can assist PSD members in the performance of their duties by introducing PSD members to each member of the official party.

(2) The attitude of the protectee is critical to the success of the PSD mission. Protectees do have a right and a responsibility to make their wishes known with respect to their personal security; they also have an obligation to listen carefully to the head of the PSD who is trained and highly qualified to assist the protectee in making reasonable judgments about manageable risks. PSD members understand their function is inherently intrusive, and that protectees can easily resent the loss of privacy that accompanies the protection offered. On the other hand, PSDs must accomplish their mission, not merely to protect executives, but to help safeguard mission critical assets - DOD executives.

(3) One of the PSD's most demanding functions is to limit the ability of individuals to circulate and approach the protectee. This is often very frustrating to protectees who wish to shake hands, engage in close conversations with visitors, and move freely without impediment in a social situation. PSDs are trained to strictly enforce limitations on the circulation of individuals, carefully checking each person for identification and ascertaining they are authorized to be present at the event.

(4) Executives with PSDs who must conduct official business or hold social engagements in large rooms can take several steps to minimize the potential disruptions that may occur as a result of good security practices.

(a) Executives should provide PSDs an attendee list prior to the function.

(b) One or more members of the executive's staff who know the attendees should be stationed with PSD members to identify the attendees as they arrive.

(c) Executive staffs should inform attendees that they shall be admitted only at specified entrances.

(d) PSD members are highly trained security specialists. While in the company of protectees, PSD members must be fully alert (no alcoholic drinks and/or drugs and medications), accommodating and helpful. Protectees should remember, however, that the PSD member's primary duty is the executive's protection, not to perform errands or to accomplish personal services for the executive. PSD members performing valet or other chores cannot effectively protect the executives.

10. Executive Protection System Integration

a. The key to successful executive protection is to ensure the level of protection afforded, by AT measures, operational procedures in the office and at home, and ~~protective security details~~PSDs, is constant. The level of protection must be matched to the threat, and must be sustainable.

b. Executives have a special responsibility to set a personal example of ~~combating~~ terrorism awareness, attention to personal, family, office, information and operations security concerns, and of AT security measures implementation. By doing so, they make their colleagues and subordinates more aware, more conscious of their security environment, and less likely to be victimized by terrorist attacks.

JURISDICTIONAL AUTHORITY FOR HANDLING TERRORIST INCIDENTS

	INITIAL RESPONSE	PRIMARY AUTHORITY/ JURISDICTION	PRIMARY ENFORCEMENT RESPONSIBILITY	EXERCISING CONTROL OF MILITARY ASSETS	PRIMARY INVESTIGATIVE RESPONSIBILITY
WITHIN THE UNITED STATES					
ON BASE	MILITARY POLICE	FBI/INSTALLATION COMMANDER	FBI/INSTALLATION COMMANDER	INSTALLATION OR UNIT COMMANDER (SUPPORT FBI)	FBI/NCIS/PMO CID/AFOSI
OFF BASE	CIVIL POLICE	FBI/CIVIL POLICE	FBI/CIVIL POLICE		FBI
OUTSIDE THE UNITED STATES					
ON BASE	MILITARY POLICE	HOST GOVERNMENT/DOS INSTALLATION COMMANDER	HOST GOVERNMENT/DOS INSTALLATION COMMANDER	INSTALLATION OR UNIT COMMANDER (IAW APPLICABLE STATUS-OF-FORCES AGREEMENT OR OTHER BILATERAL AGREEMENTS GOVERNING THE EMPLOYMENT OF MILITARY FORCES)	HOST GOVERNMENT/ NCIS/PMO CID AFOSI
OFF BASE	HOST-COUNTRY LAW ENFORCEMENT	HOST GOVERNMENT/DOS	HOST GOVERNMENT/DOS	INSTALLATION OR UNIT COMMANDER (IAW APPLICABLE STATUS-OF-FORCES AGREEMENT OR OTHER BILATERAL AGREEMENTS GOVERNING THE EMPLOYMENT OF MILITARY FORCES)	HOST GOVERNMENT WITH SUPPORT FROM US LAW ENFORCEMENT AGENCIES AS PROVIDED FOR IN BILATERAL AGREEMENTS
NOTE:	Coordinate with the local Staff Judge Advocate to clarify authority and questions of jurisdiction. Coordinate with Department of State officials as required. Coordinate in advance with local law enforcement agencies to ensure that support procedures are in place and established information/communication channels are functioning.				
LEGEND:	AFOSI FBI NCIS PMO CID DOS	Air Force Office of Special Investigations Federal Bureau of Investigation Naval Criminal Investigative Service Provost Marshal's Office Criminal Investigation Division Department of State			

Figure J-1. Jurisdictional Authority for Handling Terrorist Incidents

Intentionally Blank

APPENDIX K
REFERENCES

The development of Joint Pub 3-07.2 is based upon the following primary references:

1. Presidential Military Order of November 13, 2001, *Detention, Treatment, and Trial of Certain Non-Citizens in the War Against Terrorism*

2. Public Law 107–314—Dec. 2, 2002, *Bob Stump National Defense Authorization Act for Fiscal Year 2003*.

3. Public Law 107–296—Nov. 25, 2002, *Homeland Security Act of 2002*.

4. Statement by Mr. Paul McHale, Assistant Secretary of Defense for Homeland Defense Before the 108th Congress Senate Armed Services Committee ~~U.S.~~US Senate April 8, 2003.

5. United States Department of State, *Patterns of Global Terrorism ~~2002~~ 2003, April 2004*.

6. DOD Military Commission Order No. 1, *Procedures for Trials by Military Commissions of Certain Non-United States Citizens in the War on Terrorism*.

7. *National Strategy for Combating Terrorism*, February 2003.

8. *National Security Strategy of the USA*, September 2002.

~~8~~9. *National Strategy for Homeland Security*, July 2002.

10. *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets*, February 2003.

~~9~~11. *The ~~U.S.~~US Coast Guard Maritime Strategy for Homeland Security*, December 2002.

~~10~~12. Statements for the Record of Assistant Directors of the Federal Bureau of Investigation before House Committees and Subcommittees of the US Congress.

~~11~~13. *United States Government Interagency Domestic Terrorism Concept of Operations Plan*, January 2001.

~~12~~14. *Operational Law Handbook (2003)*.

~~13~~15. DODD 2000.12, *D~~o~~OD Antiterrorism (AT) Program*.

~~14~~16. DOD O-2000.12-H, *DOD Antiterrorism Handbook*, 9 February 2004.

~~15~~17. DODD 3020, *Defense Critical Infrastructure Protection*

~~16~~18. DODD 3025.1, *Military Support to Civil Authorities (MSCA).*

~~17~~19. DODD 3025.12, *Military Assistance for Civil Disturbances (MACDIS).*

~~18~~20. DODD 3025.15, *Military Assistance to Civil Authorities.*

21. DOD Directive 5200.27, *Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense.*

~~19~~22. DODD 5240.1, *D~~o~~OD Intelligence Activities.*

~~20~~23. DODD 5240.1-R, *Procedures Governing the Activities of D~~o~~OD Intelligence Components that Affect United States Persons.*

~~21~~24. DODI 5240.6, *Counterintelligence Awareness and Briefing Program.*

~~22~~25. DODD 5525.5, *D~~o~~OD Cooperation with Civilian Law Enforcement Officials.*

~~23~~26. DODI 2000.14, *D~~o~~OD Combating Terrorism Program Procedures.*

~~24~~27. DODI 2000.16, *D~~o~~OD Antiterrorism Standards*..25. JP 1-01, *Joint Doctrine Development System.*

28. DOD Directive 5105.62, *Defense Threat Reduction Agency.*

~~26~~28. JP 1-02, *DOD Dictionary of Military and Associated Terms.*

~~27~~29. JP 2-0, *Doctrine for Intelligence Support to Joint Operations.*

~~28~~30. JP 3-0, *Doctrine for Joint Operations.*

~~29~~31. JP 3-05, *Doctrine for Joint Special Operations.*

~~30~~32. JP 3-07, *Joint Doctrine for Military Operations Other Than War.*

~~31~~ 33. JP 3-08, *Interagency Coordination During Joint Operations.*

~~32~~34. JP 3-10, *Doctrine for Joint Rear Area Operations.*

~~33~~35. JP 3-16, *Joint Doctrine for Multinational Operations.*

~~34~~36. JP 3-26, *Joint Doctrine for Homeland Security*

~~35~~37. JP 3-54, *Joint Doctrine for Operations Security*.

~~36~~38. CJCSI 3121.01A, *Standing Rules of Engagement for US Forces (U)*.

~~37~~39. CJCSM 3122.03A, *Joint Operation Planning and Execution System Vol II, Planning Formats and Guidance*.

40. DCI Memorandum, Homeland Security Information Sharing Memorandum of Understanding, 4 March 2003 (DAC-01355-03).

41. DepSecDef Memorandum, Collection, Reporting, and Analysis of Terrorist Threats to DOD Within the United States, 2 May 2003 (U05646-03).

Intentionally Blank

APPENDIX L
ADMINISTRATIVE INSTRUCTIONS

1. User Comments

Users in the field are highly encouraged to submit comments on this publication to Commander, United States Joint Forces Command, Joint Warfighting Center, Attn: Doctrine Group, 116 Lake View Parkway, Suffolk, VA 23435-2697. These comments should address content (accuracy, usefulness, consistency, and organization), writing, and appearance.

2. Authorship

The lead agent and Joint Staff doctrine sponsor for this publication is the Director for Operations (J-3).

3. Supersession

This publication supersedes JP 3-07.2, 25 June 1993, *Joint Tactics, Techniques, and Procedures for Antiterrorism*.

4. Change Recommendations

a. Recommendations for urgent changes to this publication should be submitted:

TO: JOINT STAFF WASHINGTON DC//J34//
INFO: JOINT STAFF WASHINGTON DC//J7-JDETD//
CDRUSJFCOM SUFFOLK VA//JW100//

Routine changes should be submitted to the Director for Operational Plans and Interoperability (J-7), JDETD, 7000 Joint Staff Pentagon, Washington, DC 20318-7000 with info copy to USJFCOM JWFC (JW100).

b. When a Joint Staff directorate submits a proposal to the Chairman of the Joint Chiefs of Staff that would change source document information reflected in this publication, that directorate will include a proposed change to this publication as an enclosure to its proposal. The Military Services and other organizations are requested to notify the Director, J-7, Joint Staff, when changes to source documents reflected in this publication are initiated.

c. Record of Changes:

CHANGE NUMBER	COPY NUMBER	DATE OF CHANGE	DATE ENTERED	POSTED BY	REMARKS

5. Distribution

a. Copies of this publication can be obtained in CD format for initial distribution through the Service publication centers listed below or electronically through the Joint Electronic Library (http://www.dtic.mil/doctrine/).

b. Only approved joint publications and joint test publications are releasable outside the combatant commands, Services, and Joint Staff. Release of any classified joint publication to foreign governments or foreign nationals must be requested through the local embassy (Defense Attaché Office) to DIA Foreign Liaison Office, PO-FL, Room 1E811, 7400 Defense Pentagon, Washington, DC 20301-7400.

c. Additional copies should be obtained from the Military Service assigned administrative support responsibility by DOD Directive 5100.3, 15 November 1999, *Support of the Headquarters of Unified, Specified, and Subordinate Joint Commands*.

By Military Services:

Army:	US Army AG Publication Center SL 1655 Woodson Road Attn: Joint Publications St. Louis, MO 63114-6181
Air Force:	Air Force Publications Distribution Center 2800 Eastern Boulevard Baltimore, MD 21220-2896
Navy:	CO, Naval Inventory Control Point 700 Robbins Avenue Bldg 1, Customer Service Philadelphia, PA 19111-5099
Marine Corps:	Commander (ATTN: Publications) 814 Redford Blvd, Suite 20321 Albany, GA 31704-0321

Coast Guard:	Commandant US Coast Guard (G-OPD) 2100 2nd Street, SW Washington, DC 20593-0001
USJFCOM	Commander USJFCOM JWFC Code JW2102 Doctrine Group (Publication Distribution) 116 Lake View Parkway Suffolk, VA 23435-2697

d. Local reproduction is authorized and access to unclassified publications is unrestricted. However, access to and reproduction authorization for classified joint publications must be in accordance with DOD Regulation 5200.1-R, *Information Security Program*.

Intentionally Blank

GLOSSARY
PART I — ABBREVIATIONS AND ACRONYMS

AFOSI	Air Force Office of Special Investigations
AOR	area of responsibility
ASD/HD	Assistant Secretary of Defense for Homeland Defense
ASD(SO/LIC)	Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict)
AT	antiterrorism
ATCC	Antiterrorism Coordinating Committee
ATCC-SSG	Antiterrorism Coordinating Committee Senior Steering Group
ATEP	Antiterrorism Enterprise Portal
ATO	antiterrorism officer
CARVER	Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability
C-B	chemical-biological
CBRNE	chemical, biological, radiological, nuclear, and high yield explosives
CbT	combating terrorism
CbT RIF	combating terrorism readiness initiatives fund
CI	counterintelligence

CIA	Central Intelligence Agency
CIFA	Counterintelligence Field Activity
CISO	counterintelligence support officer; counterintelligence staff officer
CJCS	Chairman of the Joint Chiefs of Staff
COM	Chief of Mission
CONUS	Continental United States
CT	counterterrorism
CVAMP	Core Vulnerability Assessment Management Program
DCI	Director of Central Intelligence
DEST	Domestic Emergency Support Team
DHHS	Department of Health and Human Services
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DOD	Department of Defense
DODD	Department of Defense ~~D~~directive
DODI	Department of Defense ~~I~~instruction
DOE	Department of Energy
DOJ	Department of Justice
DOS	Department of State

DOT	Department of Transportation
EOC	emergency operations center
EOD	explosive ordnance disposal
EPA	Environmental Protection Agency
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FCG	Foreign Clearance Guide
FEMA	Federal Emergency Management Agency
FP	force protection
FPCON	force protection condition
HAV	Heavy Non-Tactical Armored Vehicle
H~~L~~D	homeland defense
H~~L~~S	homeland security
HN	host nation
HNS	host-nation support
HQ	headquarters
HSAS	Homeland Security Advisory System

IAW	in accordance with
IED	improvised explosive device
IPPT	Installation Antiterrorism Program and Planning Tool
IR	information requirement
J-2	~~I~~intelligence ~~D~~directorate of a joint staff
JDOMS	Joint Director of Military Support
JFC	joint force commander
~~JTF-CbT~~JITF-CT	Joint Intelligence Task Force for Combating Terrorism
JRA	joint rear area
JRAC	joint rear area coordinator
JSIVA	Joint Staff Integrated Vulnerability Assessment
JTF	joint task force
LFA	lead federal agency
MAA	
MARSEC	maritime security
MEVA	Mission Essential Vulnerable Area

MOA	memorandum of agreement
MOU	memorandum of understanding
MSHARPP	Mission, Symbolism, History, Accessibility, Recognizability, Population, and Proximity
MWD	military working dog
NCIS	Naval Criminal Investigative Service
NSC	National Security Council
NTAV	Non-Tactical Armored Vehicle
OASD(PA)	Office of the Assistant Secretary of Defense (Public Affairs)
OCONUS	outside the continental United States
OGA	other government agency
OP	observation post
OPSEC	operations security
OSD	Office of the Secretary of Defense
PA	public affairs
PAO	public affairs officer
PCA	Posse Comitatus Act

PCC	Policy Coordination Committee
~~PPBS~~ PPBE	Planning, Programming, ~~and~~ Budgeting, and Execution System
PSA	port support activity
PSD	Protective Security Details
R&R	rest & recuperation
RAM	random antiterrorism measure~~s~~
ROE	rules of engagement
~~R&R~~	~~rest & recuperation~~
SAC	special agent in charge
SecDef	Secretary of Defense
SOFA	status-of-forces agreement
SOP	standing operating procedure

TA	threat assessment
UFR	unfunded requirement
USACIDC	United States Army Criminal Investigations Command
USCG	United States Coast Guard
USD(P)	Under Secretary of Defense for Policy
USNORTHCOM	United States Northern Command
VA	vulnerability assessment
WMD	weapons of mass destruction
WMDRF	weapons of mass destruction response function
WME	weapons of mass effects

PART II — TERMS AND DEFINITIONS

antiterrorism. Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military and civilian forces. (Upon approval of the revision of this pub, this definition will be included in JP 1-02.) ~~Also called AT. (JP 1-02)~~

antiterrorism awareness. None. (Upon approval of this revision, this term and its definition will be removed from JP 1-02.)

civil support. Department of Defense support to US civil authorities for domestic emergencies, and for designated law enforcement and other activities. Also called CS. (~~Upon approval of this publication, this term and its definition will be included in JP 1-02.~~ This term and its definition are provided for information and are proposed for inclusion in the next edition of JP 1-02 by JP 3-26.)

combating terrorism. Actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts) and counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism), taken to oppose terrorism throughout the entire threat spectrum. Also called CBT. ~~(JP 1-02)~~ (This term and its definition are provided for information and are proposed for inclusion in the next edition of JP 1-02 by JP 3-40.)

consequence management. Those measures taken to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of a chemical, biological, nuclear, and/or high-yield explosive situation. For domestic consequence management, the primary authority rests with the States to respond and the Federal Government to provide assistance as required. Also called CM. See also nuclear, biological, and chemical defense. (JP 1-02)

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

counterintelligence support. Conducting counterintelligence activities to protect against espionage and other foreign intelligence activities, sabotage, international terrorist activities, or assassinations conducted for, or on behalf of, foreign powers, organizations, or persons. (JP 1-02)

counterterrorism. ~~Offensive measures taken to prevent, deter, and respond to terrorism~~ Operations that include the offensive measures taken to prevent, deter, preempt, and respond to terrorism. Also called CT. (JP 1-02)

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

DOD Elements and Personnel. – A collective term meaning DOD military and civilian personnel and their dependent family members; DOD contractors; DOD installations and facilities; DOD owned, leased, or managed infrastructure and assets critical to mission accomplishments; and other DOD-owned, leased, or managed mission essential assets overseas and in the United States, its territories, and possessions.

force protection. Actions taken to prevent or mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information. ~~These actions conserve the force's fighting potential so it can be applied at the decisive time and place and incorporate the coordinated and synchronized offensive and defensive measures to enable the effective employment of the joint force while degrading opportunities for the enemy.~~ Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease. Also called FP. (JP 1-02)

force protection condition — A Chairman of the Joint Chiefs of Staff-approved program standardizing the Military Services' identification of and recommended responses to terrorist threats against US personnel and facilities. This program facilitates inter-Service coordination and support for antiterrorism activities. Also called **FPCON.** There are four FPCONs above normal. a. **FPCON ALPHA** — This condition applies when there is a general threat of possible terrorist activity against personnel and facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of FPCON BRAVO measures. However, it may be necessary to implement certain measures from higher FPCONs resulting from intelligence received or as a deterrent. The measures in this FPCON must be capable of being maintained indefinitely. b. **FPCON BRAVO** — This condition applies when an increased and more predictable threat of terrorist activity exists. The measures in this FPCON must be capable of being maintained for weeks without causing undue hardship affecting operational capability, and aggravating relations with local authorities. c. **FPCON CHARLIE** — This condition applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel and facilities is imminent. Implementation of measures in this FPCON for more than a short period probably will create hardship and affect the peacetime activities of the unit and its personnel. d. **FPCON DELTA** — This condition applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is likely. Normally, this FPCON is declared as a localized condition. (JP 1-02)

high-risk personnel. Personnel who, by their grade, assignment, symbolic value, or relative isolation, are likely to be attractive or accessible terrorist targets. (JP 1-02)

high – yield explosive. Any conventional weapon or device that is capable of a high order of destruction or disruption and/or of being used in such a manner as to kill or injure large numbers of people. Also called HYE. (Upon approval of this revision, this term and its definition will be included in JP 1-02.)

homeland defense. ~~Homeland defense is t~~The protection of ~~U.S.~~United States territory, sovereignty, domestic population, and critical infrastructure against ~~military attacks emanating from outside the United States~~ external threats and aggression. Also called H~~L~~D. (~~Upon approval of the revision of this pub, this term and its definition will be included in JP 1-02~~This term and its definition are provided for information and are proposed for inclusion in the next edition of JP 1-02 by JP 3-26.)

homeland security. ~~Homeland security is the prevention, preemption, and deterrence of, and defense against, aggression targeted at U.S. territory, sovereignty, domestic population, and infrastructure as well as the management of the consequences of such aggression and other domestic emergencies. Homeland security is a national team effort that begins with local, state, and federal organizations. Also called HLS.~~ Homeland security, as defined in the National Strategy for Homeland Security, is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. The Department of Defense contributes to homeland security through its military missions overseas, homeland defense, and support to civil authorities. Also called HS. (~~Upon approval of the revision of this pub, this term and its definition will be included in JP 1-02~~This term and its definition are provided for information and are proposed for inclusion in the next edition of JP 1-02 by JP 3-26.)

hostage. A person held as a pledge that certain terms or agreements will be kept. (The taking of hostages is forbidden under the Geneva Conventions, 1949). (JP 1-02)

improvised explosive device. A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract. It may incorporate military stores, but is normally devised from nonmilitary components. Also called IED. (JP 1-02)

incident control point. A designated point close to a terrorist incident where crisis management forces will rendezvous and establish control capability before initiating a tactical reaction. Also called ICP. (JP 1-02)

information operations. Actions taken to affect adversary information and information systems while defending one's own information and information systems. Also called IO. (JP 1-02)

initial response force. The first unit, usually military police, on the scene of a terrorist incident. (JP 1-02)

installation. A grouping of facilities, located in the same vicinity, which support

particular functions. Installations may be elements of a base. (JP 1-02)

installation commander. The individual responsible for all operations performed by an installation. (JP 1-02)

insurgent. Member of a political party who rebels against established leadership. (JP 1-02)

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

military assistance to civil authorities. ~~Those activities and measures taken by DOD Components to foster mutual assistance and support between the Department of Defense and any civil government agency in planning or preparedness for, or in the application of resources for response to, the consequences of civil emergencies or attacks, including natural and manmade disasters, national security emergencies, and DOD assistance for civil disturbances, counterdrug, sensitive support, counterterrorism, and law enforcement. Also called MACA.~~ The broad mission of civil support consisting of the three mission subsets of military support to civil authorities, military support to civilian law enforcement agencies, and military assistance for civil disturbances. Also called MACA. (~~Upon approval of this publication, this term and its definition will be included in JP 1-02~~This term and its definition are provided for information and are proposed for inclusion in the next edition of JP 1-02 by 3-26.)

negotiations. None. (Upon approval of this revision, this term and its definition will be removed from JP 1-02.). ~~A discussion between authorities and a barricaded offender or terrorist to effect hostage release and terrorist surrender. (JP 1-02)~~

open-source intelligence. Information of potential intelligence value that is available to the general public. Also called OSINT. (JP 1-02)

operations center. The facility or location on an installation, base, or facility used by the commander to command, control, and coordinate all ~~crisis~~ operational activities. (Upon approval of this revision, this term and its definition will modify the existing term and its definition and will be included in JP 1-02.)

operations security. A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. ~~I~~identify those actions that can be observed by adversary intelligence systems. b. ~~D~~determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries. c. ~~S~~select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called OPSEC. (JP 1-02)

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

prevention. The security procedures undertaken by the public and private sector in order to discourage terrorist acts. (JP 1-02)

primary target. None. (Upon approval of this revision, this term and its definition will be removed from JP 1-02.)

proactive measures. In antiterrorism, measures taken in the preventive stage of antiterrorism designed to harden targets and detect actions before they occur. (JP 1-02)

secondary targets. None. (Upon approval of this revision, this term and its definition will be removed from JP 1-02.)

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

terrorism. The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. (~~This term and its definition replaces the existing term and its definition and is approved for inclusion in the next edition of~~ JP 1-02.)

terrorist. An individual who ~~uses violence, terror, and intimidation to achieve a result.~~ commits an act or acts of violence or threatens violence in pursuit of political, or ideological objectives. (JP 1-02)

terrorist groups. Any ~~element regardless of size or espoused cause, which repeatedly~~ number of terrorists who assemble together, have a nuifying relationship, or are organized for the purpose of commit~~s~~ing an act or acts of violence or threatens violence in pursuit of ~~its~~ their political, religious, or ideological objectives. (JP 1-02)

terrorist threat level. An intelligence threat assessment of the level of terrorist threat faced by US personnel and interests in a foreign country. The assessment is based on a

continuous intelligence analysis of a minimum of five elements: terrorist group existence, capability, history, trends, and targeting. There are five threat levels: NEGLIGIBLE, LOW, MEDIUM, HIGH, and CRITICAL. Threat levels should not be confused with force protection conditions (FPCON). Threat level assessments are provided to senior leaders to assist them in determining the appropriate local FPCON. (Department of State also makes threat assessments, which may differ from those determined by Department of Defense.) (JP 1-02)

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

threat and vulnerability assessment. In antiterrorism, the pairing of a facility's threat analysis and vulnerability analysis. (JP 1-02)

vulnerability assessment. A Department of Defense, command, or unit-level evaluation (assessment) to determine the vulnerability of a terrorist attack against an installation, unit, exercise, port, ship, residence, facility, or other site. Identifies areas of improvement to withstand, mitigate, or deter acts of violence or terrorism. (JP 1-02)

weapons of mass destruction. — A ~~W~~weapons that ~~are~~ is capable of a high order of destruction and/or of being used in such a manner as to destroy large numbers of people. Weapons of mass destruction can be high explosives or nuclear, biological, chemical, and radiological weapons, but exclude the means of transporting or propelling the weapon where such means is a separable and divisible part of the weapon. Also called WMD. (Upon approval of this revision, this term and its definition will modify the existing term and its definition and will be included in JP 1-02.)

~~**weapons of mass effects**. A single system or device that can create large scale (over 1 km2 area, and/or result in hundreds to thousands of material or personnel "casualties") detrimental (lethal or non-lethal, including economic) effects to military or civilian operations . Also called WME. (Upon approval of the revision of this pub, this term and its definition will be included in JP 1-02.)~~

Intentionally Blank


JOINT
CHIEFS OF STAFF